Préface

Le 25 mai 2018 entrera en vigueur le Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après, le RGPD). Il remplacera à cette date la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, qui régit actuellement la matière et dont la transposition est assurée en Belgique par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Le premier considérant du RGPD rappelle que la protection des personnes physiques à travers le traitement de leurs données à caractère personnel est un droit fondamental qui trouve sa source à l'article 8, § 1er, de la Charte des droits fondamentaux de l'Union européenne et à l'article 16, § 1er, du Traité sur le fonctionnement de l'Union européenne. La protection des données personnelles s'inscrit ainsi dans le cadre plus large de la protection de la vie privée et familiale, du domicile et de la correspondance, notamment consacrée par l'article 8 de la Convention européenne des droits de l'homme et, en droit interne, par l'article 22 de notre Constitution.

En effet, à côté de la protection du droit à la vie privée, est apparue une nouvelle forme de protection des individus, la protection des données les concernant qui est plus récente. Elle est notamment liée aux développements informatiques et aux risques collatéraux inhérents à ceux-ci. C'est d'ailleurs, entre autres, pour s'adapter aux nouvelles technologies et notamment aux Facebook, Twitter, LinkedIn, MySpace, YouTube, Snapchat et autres médias sociaux que le RGPD a été rédigé au niveau européen. Les auteurs du RGPD avaient pour objectif de moderniser le texte de la directive pour tenir compte des nouvelles technologies et notamment des médias sociaux et de leur impact sur la vie privée des personnes concernées. Ils voulaient aussi harmoniser les règles existant au niveau européen afin que la protection offerte soit comparable, mais surtout que les limites floues de la vie privée soient comprises et appréhendées d'une manière uniforme partout dans l'Union européenne. Le RGPD témoigne de la volonté politique à tous les niveaux de mieux protéger la vie privée des individus dans une société où le concept de vie privée ne cesse de s'élargir et, donc paradoxalement, d'échapper à toute tentative de définition. Le vote laborieux des dispositions du RGPD, après des années de négociation, s'est accompagné

de nouvelles règles permettant au citoyen de mieux maîtriser le contrôle de ses données personnelles, avec comme corollaire, une série d'obligations à charge des responsables de traitement et des sous-traitants.

La protection de la vie privée et celle des données des personnes physiques est indissociable de nos jours de toute activité économique. Nous vivons, en effet, dans une société numérique dans laquelle les données personnelles constituent une nouvelle valeur, qu'il convient de traiter et protéger efficacement.

La mise en œuvre du nouveau RGPD constitue un enjeu important pour les entreprises. Il ne faut pas sous-estimer la charge administrative en temps, en argent, en ressources humaines que cela représente. Aussi lourde soit-elle, cette tâche est nécessaire, je dirais même inéluctable, dans un monde numérique où les données s'échangent, s'achètent et se vendent et sont liées à toutes les activités des entreprises, de la gestion du personnel aux contacts clients et prospects en passant notamment par les activités marketing, statistiques, CRM, …

Le RGPD peut également être envisagé comme une opportunité pour les entreprises : opportunité commerciale car c'est l'occasion de contacter ses clients et de leur montrer que l'entreprise joue la carte de la transparence dans l'esprit du RGPD, atout concurrentiel en présentant sa conformité au RGPD avant d'autres entreprises concurrentes et enfin, réputationnel en se montrant « RGPD *compliant* ».

Si toutes les entreprises n'utilisent pas des données dites sensibles ou n'ont pas pour activité principale (*core business*) la gestion de données à caractère personnel, il n'empêche que toutes traitent des données en tant que responsable de traitement ou en tant que sous-traitant et doivent donc intégrer la notion de protection des données dans leurs activités. Cette nouvelle protection est intrinsèquement liée à toute activité, à tout traitement de données. Le RGPD doit dorénavant faire partie de l'ADN de l'entreprise, il est intimement lié au choix des finalités, des données traitées, des mesures de sécurité mises en place…

Les principes fondamentaux de toute législation relative aux traitements de données à caractère personnel et du RGPD en particulier (droit d'accès, principe de finalité…) participent à la construction d'un système de protection qui recherche un équilibre entre des intérêts et des libertés qui s'opposent. Ce difficile équilibre est mis en exergue par le contentieux de plus en plus fourni où se mêlent des questions aussi diverses que la publication d'une photo indiscrète de nos têtes couronnées ou stars de nos petits écrans, la perquisition d'un cabinet d'affaires, la plainte d'une personne non informée de la cession de ses données par une entreprise commerciale à une autre, etc.

À l'ère de la société ultra-connectée, la tentation de collecter et de recouper un nombre toujours plus important de données personnelles est grande. Pour s'en prémunir, il faut passer par un double garde-fou : d'une part, le principe de finalité des données collectées et, d'autre part, celui de proportionnalité des intérêts.

La méthode de pondération des intérêts est la clé de voûte qui permet un équilibre entre les intérêts des parties concernées. Le RGPD entend définir certains critères qui permettent de préciser le droit au traitement de l'information du responsable de traitement, expression tantôt de sa liberté d'entreprendre dans le secteur privé, tantôt de son rôle de gardien de l'intérêt général dans le secteur public. L'exigence de pondération des intérêts est au centre du débat de la notion de vie privée. « Le concept juridique de vie privée ne saurait donner lieu à une application syllogistique permettant d'identifier par une opération purement logique la situation appréhendée par le concept de vie privée. La méthode de pondération des intérêts est la seule appropriée. »[1] Dans le secteur privé, le service attendu de l'entreprise collectrice de données est à la fois la justification et la limite de l'usage des renseignements.

Comme on peut rapidement le comprendre, le RGPD n'est pas un texte facile à appréhender, encore moins à mettre en œuvre au sein d'une entreprise quelle que soit sa taille et son activité. C'est ainsi que le RGPD a, dès à présent, été à l'origine de l'organisation d'un grand nombre de formations, de séances de sensibilisation, de consultations juridiques et que les articles le concernant dépassent largement tout autre domaine. Il concerne tout le monde, entreprises et personnes physiques, secteur public et secteur privé.

Dès janvier 2016, la FEB a pris le parti de sensibiliser le monde des entreprises et de l'informer des nombreuses facettes et domaines que le RGPD impacte. Elle a publié une brochure et un ouvrage reprenant les actes des différents ateliers pratiques qu'elle a organisés en 2016[2]. Il est indispensable d'aider les entreprises dans le dédale des 99 articles et des considérants y relatifs du RGDP ainsi qu'au travers des guidelines du Groupe 29 qui sont très peu explicites et manquent de clarté. Je salue donc cet ouvrage très pratique qui pourra servir de guide à toutes les entreprises soucieuses de comprendre les dispositions du RGPD qui s'imposent à elles, même si elles font appel à un Data Protection Officer externe ou à un avocat ou consultant. Les fiches de guidance seront pour tous, juristes ou non, l'outil de référence pour les guider dans la voie de la mise en conformité et de leur *accountability*. Gérer la protection des données de votre entreprise constitue un élément important dans le cadre de vos activités. Il en va de votre réputation.

Philippe LAMBRECHT
Administrateur-Secrétaire Général FEB

1. F. Rigaux, *La protection de la vie privée et autres biens de la personnalité*, Bruxelles, Bruylant, 1990, p. 770.

2. Data Protection & Privacy, Le GDPR dans la pratique, Anthemis, 2017.

Avant-propos

L'entrée en vigueur du règlement européen sur la protection des données constitue assurément un bouleversement pour la plupart des entreprises qui, jusqu'à présent, n'avaient pas, ou très peu appréhendé cette problématique.

Pourtant, cette matière n'est pas neuve et au final, bon nombre de concepts présents dans le RGPD étaient déjà existants dans la réglementation précédente. La pratique démontrait toutefois que cette matière était très peu respectée, voire prise en compte par les acteurs économiques.

Comme tout nouveau bouleversement (ou prise de conscience ?), cela implique une modification radicale des mentalités de l'entreprise, et surtout des pratiques tant vis-à-vis des personnes extérieures que vis-à-vis des personnes concernées au sein même de l'entreprise à savoir les employés, les collaborateurs externes, etc.

Ce changement apporte également son lot, presque quotidien, de croyances erronées autour du sujet, et de confusions parfois tenaces.

Pour le juriste ou même l'apprenti DPO, confronté à la mise en pratique de cette matière, le premier travail est sans aucun doute un travail de démystification et de compréhension des concepts tant juridiques que techniques.

Il faut détruire les croyances erronées, sensibiliser, dédramatiser, … Il y a, dans l'entrée en vigueur du RGPD, presque une approche psychologique importante, ce d'autant plus que bon nombre d'acteurs brandissent les sanctions comme fer-de-lance pour la mise en conformité des entreprises.

L'ouvrage de Monsieur Axel BEELEN constitue une synthèse claire, précise et pragmatique des divers concepts exposés dans le cadre du règlement général de la protection des données.

Avec ces fiches de guidance, impossible de se perdre dans les méandres de la protection des données.

L'ouvrage a également le mérite de donner aux juristes des clés de compréhension efficaces pour mettre en pratique cette matière et guider les entreprises sur le chemin de la mise en conformité qui ne s'arrêtera certainement pas le 25 mai 2018.

Frédéric DECHAMPS

Avocat, Lex4u

Objectif de l'ouvrage

Introduction

Le Règlement Général sur la Protection des Données pour RGPD et en anglais *General Data Protection Regulation* pour GDPR est un nouveau règlement européen entré en vigueur en mai 2016, mais dont l'application a été différée de deux ans, au 25 mai 2018.

Le RGPD concerne la réglementation des données à caractère personnel (ou données personnelles parfois dans la suite de l'ouvrage) dans l'Union européenne. Comme il s'agit d'un Règlement, il va s'appliquer directement et automatiquement dans les 28 (bientôt 27 ?) États de l'Union à la date du 25 mai 2018.

Beaucoup d'articles et d'ouvrages vous le rappellent constamment (les meilleurs étant évidemment publiés aux Éditions Larcier) : il est plus que temps que vous commenciez votre travail de mise en conformité avec ce texte hautement important. La mise en conformité ne s'arrêtera pas au 25 mai 2018. En effet, l'ensemble de vos activités devra respecter toujours cette complexe réglementation.

Nous avons voulu ici vous aider dans vos analyses au travers de Fiches de guidance pratiques. Nous avons inclus dans l'ouvrage les dernières recommandations officielles (dont celles notamment du Groupe de Travail « Article 29 »). Mais nul doute que d'autres viendront encore.

Structure de l'ouvrage

Première partie

Dans la première partie du livre, vous trouverez des Fiches de guidance consacrées à différents articles du RGPD. Les parties les plus importantes du RGPD sont ainsi parcourues et expliquées pour vous au travers de mots simples et d'explications que nous avons voulues aussi claires que possible.

L'ensemble de nos Fiches de guidance vous permettront aisément de savoir ce que recouvrent les concepts d'*accountability* (Fiche de guidance n° 4), de *privacy by design* et de *privacy by default* (Fiche de guidance n° 5),

que doit contenir mon registre des activités de traitement (Fiche de guidance n° 8), dois-je obligatoirement nommer un Délégué à la Protection des Données (Fiche de guidance n° 11), quels sont les droits (nouveaux et anciens) des personnes concernées (Fiche de guidance n° 16 à 25), devrais-je notifier à l'autorité de contrôle toutes les violations de données personnelles (Fiche de guidance n° 26), etc.

Seconde partie

Dans la seconde partie du livre, vous trouverez des Fiches de guidance sur des thèmes liés au RGPD.

En effet, la problématique de la protection des données à caractère personnel est très actuelle.

La matière est transversale, moderne et tentaculaire.

Elle a des liens avec les règles qui gouvernent la protection des données issues des communications électroniques (Fiche de guidance n° 37) ou avec celles que vous retrouvez dans la directive NIS (Fiche de guidance n° 40).

Les questions autour de la protection des données personnelles impactent le quotidien des entreprises comme lorsqu'elles désirent réaliser des campagnes de marketing direct (Fiche de guidance n° 44) basées sur un profilage (Fiche de guidance n° 25) réalisé grâce à un très bon big data (Fiche de guidance n° 35) ou stocker leurs données dans le cloud (Fiche de guidance n° 42).

Le RGPD ne devra également pas être oublié par les start-ups ou par les sociétés qui développent des objets connectés (Fiche de guidance n° 36) ou leur propre blockchain (Fiche de guidance n° 45).

Nul doute que d'autres sujets viendront très vite compléter nos analyses. Nous en avons listés les principaux dans notre dernière Fiche de guidance (la n° 46).

Présentation

Les Fiches sont à chaque fois présentées de la même façon :

1. Leur titre ;
2. Les articles et les considérants du RGPD concernés ;
3. Notre commentaire ;
4. Un renvoi vers les Lignes directrices du Groupe de Travail « Article 29 » et vers les Fiches de guidance liées.

Vous trouverez en fin d'ouvrage plusieurs Annexes (dont deux Fiches de guidance bonus !).

Les fiches se veulent pratiques et complémentaires aux ouvrages auxquels nous vous renvoyons en fin de livre.

Conventions

Nous avons préféré utiliser les termes français de la matière. Nommons ici leur correspondance en anglais car vous les trouverez souvent dans la pratique des affaires :

1. Analyse d'impact relative à la protection des données (AIPD) : *Data Protection Impact Assessment (DPIA)*
2. Délégué à la Protection des Données (DPD) : *Data Protection Officer (DPO)*
3. Finalité : *Purpose*
4. Personne concernée : *Data Subject*
5. Principe général de responsabilité à la charge du Responsable de traitement : *Accountability*
6. Protection des données dès la conception : *Protection by Design*
7. Protection des données par défaut : *Protection by Default*
8. Registre des activités de traitement : *Record of Processing Activities*
9. Règlement Général sur la Protection des Données (RGPD) : *General Data Protection Regulation (GDPR)*
10. Règles d'entreprises contraignantes : *Binding Corporate Rules (BCR)*
11. Responsable du traitement : *Data Controller*
12. Sous-traitant : *Data Processor*

Bonne lecture !

Le manuscrit a été terminé le 28 mars 2018.

Axel Beelen (@ipnewsbe)

Fiche de guidance n° 1
Le champ d'application matériel du RGPD

Article 2 du RGPD

Considérants 14 à 21 du RGPD

A. Quels types de données sont concernées par le RGPD ?

Le RGPD concerne le traitement de données à caractère personnel (parfois abrégées en « données personnelles » et confondues souvent avec les « *Personally Identifiable Information* », les PII).

Une donnée à caractère personnel est toute information se rapportant à une personne physique identifiée ou identifiable.

Il s'agit de toute information ou donnée qui peut identifier directement ou indirectement via un recoupement par exemple une personne physique. Il peut s'agir d'un identifiant, tel qu'un nom patronymique, une date de naissance, un numéro d'identification, des données de localisation, un identifiant en ligne, une adresse email, d'un ou plusieurs éléments spécifiques propres à l'identité physique (une empreinte digitale), physiologique, génétique, psychique, économique, culturelle ou sociale de la personne concernée.

Une donnée qui ne semble pas à première vue permettre d'identifier une personne physique lorsqu'elle est liée ou croisée avec d'autres sources est aussi une donnée à caractère personnel tombant sous le champ d'application du RGPD.

La Cour de justice de l'Union européenne a une interprétation très large de ce qu'il faut entendre par « données personnelles ». Elle a, par exemple, considéré dans une décision rendue fin décembre 2017 que : « Les réponses écrites fournies lors d'un examen professionnel et les éventuelles annotations de l'examinateur relatives à ces réponses constituent des données à caractère

personnel du candidat auxquelles il a, en principe, un droit d'accès » (arrêt du 20 décembre 2017, aff. C-434/16). Elle avait précédemment déjà jugé le 19 octobre 2016 (affaire C-582/14) qu'une adresse de protocole Internet dynamique est également une donnée à caractère personnel.

Vous êtes concerné par le RGPD si l'un de vos services, ou un de vos sous-traitant, traite, gère, utilise et/ou dispose de données à caractère personnel.

Et c'est plus fréquent qu'on ne le pense. Quelques exemples de traitement ?

- Le fichier des lecteurs de la bibliothèque communale
- La liste des abonnés au centre culturel
- La liste des enfants inscrits dans les crèches communales ou aux activités extra-scolaires
- Les dossiers de patients d'une maison médicale ou d'un home
- Les données conservées électroniquement ou sur papier par les Ressources Humaines
- La liste des personnes à qui vous envoyez une newsletter électronique ou papier
- Les coordonnées de candidats à un logement social, à une allocation de remplacement
- Toutes les demandes de citoyen en vertu d'une réglementation (permis d'urbanisme, passeport, …)

La conformité de toute entreprise devra concerner tant les données structurées que les données non structurées du moment que ces données sont des données à caractère personnel. Les données non structurées concernent toutes les informations (en ce compris donc les données à caractère personnel qui y sont incluses) qui se retrouvent dans les documents (documents Word, emails, tableaux de chiffres, vidéos, textes, images, pages web, réseaux sociaux, etc.) que nous enregistrons sur nos serveurs, dans nos disques durs, etc. sans les classer véritablement.

Les données non structurées ont aussi leur part d'inconnu. Formats variés, volumes gigantesques, production en continu et niveaux de criticité hétérogènes… Pourtant, ces données sont un enjeu majeur pour les entreprises car, une fois organisées et analysées méthodiquement, ces données recèlent énormément de valeur. Mais il est clair aussi qu'organiser et protéger ces données peut représenter une tâche herculéenne.

Le RGPD ne couvre pas le traitement des données qui concernent les personnes décédées ou les personnes morales.

Une société devra respecter les règles du RGPD durant toute la durée de vie d'une donnée personnelle :

- de sa collecte ;
- à sa destruction ;
- en passant par chaque transfert de la donnée ;

- chaque accès à celle-ci ;
- chaque manipulation et
- chaque enregistrement.

B. Qu'entend-on par « traitement de données » ?

Un traitement est toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel.

L'article 4.2 du RGPD cite en exemple la collecte (il s'agira du cas le plus courant) (la collecte pouvant se réaliser en ligne ou bien lors d'un entretien de visu), l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation (la simple consultation même à distance depuis un autre pays de données personnelles est bel et bien un traitement de données), l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Le RGPD s'applique :

1. au traitement de données à caractère personnel, automatisé en tout ou en partie (notez la neutralité technologique rappelée par le considérant 15 du RGPD),
2. au traitement non automatisé (= les traitements manuels) de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Les données à caractère personnel traitées doivent être contenues ou appelées à figurer dans un fichier.

Un « fichier » est un ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique. Les dossiers ou les ensembles de dossiers qui ne sont pas structurés selon des critères déterminés ne relèvent donc pas du champ d'application du RGPD.

Le RGPD ne s'appliquera également pas aux traitements de données à caractère personnel effectués :

1. dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union européenne par exemple en matière de sécurité nationale ;
2. par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne (politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration) ;

3. par une personne physique dans le cadre d'une activité strictement personnelle ou domestique et qui n'ont donc aucun lien avec l'activité professionnelle de la personne physique.

   Le considérant 18 du RGPD cite en exemple les « échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités ». Toutefois, le RGPD s'appliquera bien aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques. La gestion de vos emails personnels par Outlook ne relève pas du RGPD. Par contre, Microsoft sera bien lui soumis au RGPD car il réalise des activités de traitements sur des données personnelles ;

4. relatifs à des personnes décédées ;

   Toutefois, les États membres peuvent déroger à ce principe et prévoir des règles relatives au traitement des données à caractère personnel des personnes décédées (il faudra voir si la Belgique lèvera cette option ou pas) (à titre d'illustration, de telles règles sont prévues en droit français : droit pour les personnes concernées de définir des directives générales et particulières pour le traitement de leurs données post-mortel notamment) ;

5. par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

C. Qu'entend-on par « responsable du traitement » ?

Selon l'article 4.7 du RGPD, un « responsable du traitement » est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

Dans l'important arrêt *Google Spain* du 13 mai 2014 (aff. C-131/12), la Cour de justice de l'Union européenne a précisé que :

1. l'opération consistant en l'exploration de manière automatisée, constante et systématique d'Internet à la recherche des informations qui y sont publiées, est à qualifier de traitement.

En effet, l'exploitant d'un moteur de recherche à ce moment « collecte » de telles données qu'il « extrait », « enregistre » et « organise » par la suite dans le cadre de ses programmes d'indexation, « conserve » sur ses serveurs et, le cas échéant, « communique à » et « met à disposition de » ses utilisateurs sous forme de listes des résultats de leurs recherches ;

2. c'est l'exploitant du moteur de recherche qui détermine les finalités et les moyens de cette activité et ainsi du traitement de données à caractère personnel qu'il effectue, lui-même, dans le cadre de celle-ci et qui doit, par conséquent, être considéré comme le « responsable » de ce traitement.

D. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

➟ *Fiche de guidance n° 2 : Le champ d'application territorial du RGPD*

Fiche de guidance n° 2
Le champ d'application territorial du RGPD

Article 3 & 27 du RGPD

Considérants 27 à 34 & 80 du RGPD

A. Introduction

Il existe plusieurs sources de référence pour organiser la protection des données à caractère personnel et leur transfert par grandes zones géographiques.

En voici quelques-unes :

1. les recommandations de l'OCDE ;
2. les *Cross Border Privacy Rules* dans la région Asie-Pacifique ;
3. la Convention n° 108 du Conseil de l'Europe, qui est une référence pour tous les pays signataires, dont la Russie ;
4. le Règlement européen sur la protection des données personnelles (RGPD) ;
5. le *Privacy Shield* qui encadre une partie des transferts entre l'Europe et les États-Unis.

Par rapport à la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, le champ d'application territorial des nouvelles règles européennes a été étendu pour avoir véritablement un champ d'application extraterritorial.

Certains l'ont même surnommé le « *Global* » *Data Protection Regulation* vu ses impacts juridiques très nombreux.

B. Deux possibilités sont à envisager

1. Le responsable du traitement ou le sous-traitant a un établissement stable dans l'UE

Le RGPD s'applique aux traitements des données à caractère personnel effectués dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant situé sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union européenne.

L'article 3 du RGPD qui reprend cette règle de la Directive de 1995 étend donc dorénavant le champ d'application territoriale du RGPD aux traitements réalisés par un sous-traitant établi sur le territoire de l'Union européenne que le traitement ait lieu ou non dans l'Union. Il s'agit d'une grande nouveauté par rapport à la Directive de 1995 qui ne prévoyait aucune règle pour le sous-traitant.

Notion d'établissement

Si la notion d'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable, la forme juridique de cet établissement n'est pas déterminante (il peut s'agir d'une simple succursale ou au contraire d'une filiale disposant de la personnalité juridique).

2. Quid si le responsable du traitement ou le sous-traitant n'a pas un établissement stable dans l'UE ?

Dorénavant, le RGPD s'appliquera aux traitements des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union européenne (qu'importe leur nationalité) par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union européenne dans le cas où leurs activités de traitement sont liées (deux possibilités) :

1. à l'offre de biens ou de services à ces personnes concernées lorsque ces dernières se trouvent sur le territoire de l'Union, qu'un paiement soit exigé ou non (même gratuitement donc car souvent, on paie ces services gratuits par la communication et l'autorisation de traiter nos données personnelles) desdites personnes ou
2. au suivi du comportement de ces personnes (profilage), dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union européenne.

Notion d'offre de biens ou de services à des personnes concernées au sein de l'Union

La simple accessibilité du site internet d'une entité depuis le territoire de l'Union européenne ne suffit pas pour considérer que ce site offre des biens ou des services à des personnes concernées se trouvant dans l'Union européenne. En revanche, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs pays de l'Union européenne, avec la possibilité de commander des biens ou services dans cette langue, ou la référence sur le site internet à des clients ou utilisateurs établis dans l'Union européenne, peuvent indiquer que des biens ou services sont proposés à des personnes concernées dans l'Union européenne.

Notion de suivi du comportement

À titre d'exemple, un suivi des internautes dans le cadre de leur navigation sur le web, couplé avec des techniques de traitement visant à déterminer un profil, notamment afin de prendre des décisions ou d'analyser leurs préférences de consommation, leurs comportements, etc. répond à la notion de suivi du comportement de ces personnes.

Le RGPD s'applique aussi au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.

Si la société (qu'elle soit responsable du traitement ou sous-traitant) n'est pas établie dans l'UE mais qu'elle doit donc malgré tout respecter le RGPD, elle devra désigner par écrit un représentant qui sera le point de contact pour les autorités de contrôle des données personnelles (article 27 du RGPD).

Le représentant désigné est établi dans un des États membres dans lesquels se trouvent les personnes physiques dont les données à caractère personnel font l'objet d'un traitement lié à l'offre de biens ou de services ou dont le comportement fait l'objet d'un suivi.

Le représentant est mandaté par le responsable du traitement ou le sous-traitant pour être la personne à qui, notamment, les autorités de contrôle et les personnes concernées doivent s'adresser, en plus ou à la place du responsable du traitement ou du sous-traitant, pour toutes les questions relatives au traitement, aux fins d'assurer le respect du RGPD

La désignation d'un représentant par le responsable du traitement ou le sous-traitant est sans préjudice d'actions en justice qui pourraient être intentées contre le responsable du traitement ou le sous-traitant lui-même.

Une entité non établie dans l'UE sera dispensée de désigner un représentant dans le cas où :

a) elle réalise un traitement qui est occasionnel et qui n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement ;

b) elle réalise un traitement qui n'implique pas un traitement à grande échelle des catégories particulières de données visées à l'article 9.1 ou 10 du RGPD et qui n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement ;

c) il s'agit d'une autorité publique ou d'un organisme public.

Rappelons qu'en application de l'article 4 de la Directive 95/46/CE relatif au droit national applicable, l'application de la loi nationale d'un État membre de l'Union européenne à un responsable de traitement qui n'y était pas établi supposait qu'il ait recours « […] à des moyens, automatisés ou non, situés sur le territoire dudit État membre […] ».

Cette notion était entendue de manière large afin de soumettre une très grande partie des responsables de traitement à la loi de protection d'un État membre. Aussi les moyens de traitement pouvaient être caractérisés uniquement par des logiciels de collecte utilisés, des formulaires de collecte, des serveurs informatiques ou encore le recours à des cookies. Toutefois, cela posait de nombreux problèmes d'interprétation. La clarification apportée ici par le RGPD est plus que bienvenue.

Il reste maintenant à voir comment concrètement les autorités de contrôle nationales et le futur Contrôleur Européen de la Protection des Données (CEPD) pourront exercer un réel contrôle sur les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) et autres souvent situés aux États-Unis mais qui se moquent bien des règles européennes.

C. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

➠ *Fiche de guidance n° 1 : Le champ d'application matériel du RGPD*

Fiche de guidance n° 3
Les principes généraux de protection des données

Articles 5, 6.4 & 11.1 du RGPD

Considérants 39 à 50, 57 & 157 du RGPD

A. Introduction

L'article 5 du RGPD contient les principes généraux et essentiels qui doivent guider tout traitement relatif à des données à caractère personnel.

Rajoutons aux six principes de l'article 5, le principe de transparence. En effet, il traverse toute la compréhension du RGPD.

Ce dernier principe s'applique principalement :

1. lorsque le responsable du traitement doit fournir des informations aux personnes concernées à propos de ses activités de traitement.

   Le responsable devra toujours vérifier la bonne compréhension des informations qu'il fournit et ce en fonction de son public cible ;
2. lorsque le responsable du traitement communique avec les personnes concernées à propos de l'exercice de droits ou d'une violation de données à caractère personnel ;
3. quand le responsable du traitement doit faciliter l'exercice par les personnes concernées de leurs droits.

Ce principe fondamental (voire le plus important de toute la matière) permet de donner de la confiance aux personnes concernées en leur permettant de comprendre et d'appréhender convenablement les activités de traitement du responsable du traitement et, s'ils le souhaitent, de demander plus d'informations, de s'y opposer, de retirer leur consentement, etc.

Cette obligation de transparence est explicitée au considérant 39 du RGPD :

« Le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées.

Le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples.

Ce principe vaut, notamment, pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement. »

B. Les principes

Selon l'article 5 du RGPD, les données à caractère personnel doivent être :

1. traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence).

   La licéité du traitement fait référence à son fondement juridique tandis que la loyauté du traitement désigne les modalités selon lesquelles les données sont collectées (lien avec le principe de transparence et avec l'information à fournir aux personnes concernées au moment de la collecte de leurs données) ;

2. collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (limitation des finalités).

   Les responsables des traitements devront toujours définir au préalable le but poursuivi et ce de manière claire, afin que les finalités arrêtées puissent être facilement comprises par les personnes concernées (principe de transparence). Cette étape revêt une importance particulière puisqu'elle limitera par la suite les éventuelles réutilisations des données personnelles. Notez que le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales ;

3. adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données, ancien principe dit de proportionnalité).

   Il s'agit ici de préciser que le responsable de traitement ne peut traiter des données personnelles à moins d'y être contraint et après avoir

vérifié l'inexistence de procédures alternatives permettant d'atteindre un résultat identique ou similaire sans traitement de données personnelles. Le principe de minimisation permettra aussi de prévenir d'éventuelles utilisations délictuelles et d'optimiser les coûts et les frais liés au respect de la conformité.

Les entreprises ne peuvent collecter et traiter des données à caractère personnel que si l'objectif recherché rend cette collecte et ce traitement vraiment indispensables. Si la collecte de données est indispensable pour parvenir à un certain objectif, alors, l'entreprise peut (si toutes les autres conditions du RGPD sont remplies) collecter et traiter les données mais uniquement les données strictement nécessaires à la finalité poursuivie. La minimisation vise donc tant l'étendue, la quantité que le caractère nécessaire des données traitées.

À titre d'illustration : une entreprise qui propose sur son site internet aux internautes de recevoir gratuitement un devis ou toute autre documentation, peut recueillir l'identité et les coordonnées du demandeur pour répondre à sa demande, mais ne doit en aucun cas collecter ses coordonnées bancaires même s'il s'agit uniquement d'anticiper des relations futures ;

4. exactes et, si nécessaire, tenues à jour.

   Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (principe d'exactitude des données). Le responsable du traitement devra mettre en place des processus permettant d'effectuer une revue régulière des données afin de déterminer si elles sont encore pertinentes ou au contraire devenues obsolètes, etc. ;

5. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

   Les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le RGPD afin de garantir les droits et libertés de la personne concernée (limitation de la conservation).

   La durée de conservation limitée des données sera un enjeu important pour le responsable de traitement car elle devra désormais figurer dans la mention d'information délivrée aux personnes concernées. Dès lors, ces dernières seront en mesure de vérifier si l'organisme responsable de traitement respecte la durée qu'il a lui-même au préalable déterminée et communiquée.

D'un point de vue pragmatique, une véritable politique de conservation, d'archivage et de purge des données devra être formalisée ;

6. traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

   La mise en œuvre de ces mesures doit notamment passer par la formalisation d'une politique de sécurité des données, d'actions de sensibilisation des membres du personnel, etc.

C. Traitement secondaire

Imaginons qu'un responsable du traitement souhaite utiliser (traiter) des données précédemment collectées pour une finalité différente de la finalité initiale. Il pourra bien sûr rechercher un nouveau consentement de la part des personnes concernées. Il se pourrait aussi que le droit de l'Union ou le droit d'un État membre permette expressément cet autre traitement.

Dans le cas où le traitement second n'est pas fondé sur le consentement ou le droit de l'Union ou de l'État membre, le responsable du traitement devra déterminer si la finalité du traitement ultérieur est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées.

Afin de déterminer si le traitement ultérieur et à une autre fin est bel et bien compatible, le responsable du traitement devra tenir compte, entre autres,

a) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;

b) du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;

c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10 du RGPD ;

d) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;

e) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

Ce changement de finalité possible permet d'assouplir en quelque sorte le principe de finalité posé à l'article 5 du RGPD.

Si les finalités pour lesquelles des données à caractère personnel sont traitées n'imposent pas ou n'imposent plus au responsable du traitement d'identifier une personne concernée, le responsable n'est pas tenu de conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le RGPD.

D. Le respect du RGPD repose sur les épaules du responsable du traitement

Le responsable du traitement est responsable du respect de ces principes généraux. Il doit être constamment en mesure de démontrer que ceux-ci sont respectées à tout instant (principe de responsabilité ou d'« *accountability* »).

En pratique

Les entreprises vont devoir agir et être en mesure de prouver, de tracer, ce qui a été fait. Cela passera notamment par l'implémentation de documentations adaptées et de politiques de traitement des données écrites et contraignantes, ou encore de procédures de vérifications (régulièrement testées) pour s'assurer de l'effectivité et de l'efficacité des mesures mises en œuvre pour le respect des dispositions applicables.

Le RGPD définit le responsable du traitement comme toute personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Notion centrale et faisceau d'indices

S'agissant de l'identification du responsable de traitement, une analyse au cas par cas, *in concreto*, doit être menée pour tout traitement mis en œuvre dans la mesure où cette notion est centrale. En effet, il s'agit de l'entité sur laquelle repose les principales obligations en matière de protection des données à caractère personnel.

À cet égard, divers critères et indices doivent être pris en compte afin de déterminer l'entité devant être qualifiée de responsable de traitement : initiative du traitement et définition de la finalité/des objectifs, influence de droit ou de fait sur le traitement et degré d'influence, autonomie et pouvoir décisionnaire, image donnée aux personnes concernées et attentes raisonnables que cette visibilité peut susciter chez ces dernières, détermination des moyens matériels, humains, techniques et organisationnels du traitement, etc.

Le règlement est également applicable aux entités qui traitent les données en qualité de sous-traitant, c'est-à-dire qui traitent les données pour le compte d'un tiers, lui-même responsable de traitement.

En effet, si le sous-traitant agit par définition uniquement pour le compte (et donc sur instruction) du responsable de traitement, certaines obligations spécifiques, voire stratégiques, sont tout de même mises à sa charge par le règlement.

Nous rappellerons constamment les principes généraux lorsque nous analyserons les différents chapitres du RGPD. Il faut en effet toujours les garder à l'esprit. Ils soutiennent toute interprétation de la nouvelle réglementation.

E. Les Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail « Article 29 » a adopté des Lignes directrices en rapport avec l'obligation de transparence du responsable du traitement (disponibles uniquement en anglais pour l'instant sur le site internet du Groupe de Travail) (« *Guidelines on transparency under Regulation* 2016/679 », Réf. WP 260).

Ces Lignes directrices sont soumises à consultation jusqu'au 23 janvier 2018. La version finale sera publiée par après.

F. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 4 : L' « accountability »*
- *Fiche de guidance n° 6 : Le consentement*
- *Fiche de guidance n° 16 : Les modalités d'exercice des droits des personnes concernées*
- *Fiche de guidance n° 18 : Droit 1 : Le droit d'information des personnes concernées*

Fiche de guidance n° 4
L'« *accountability* »

Article 5.2 du RGPD

Considérants 50 & 157 du RGPD

A. Principe

Il s'agit d'une des grandes nouveautés du RGPD par rapport à la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

L'accountability désigne l'obligation pour les entreprises de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que ses traitements des données à caractère personnel sont effectués conformément au règlement, et être en mesure de le démontrer. Les entreprises devront appliquer l'ensemble des principes établis par le RGPD, respecter les obligations qui en découlent, s'en assurer constamment et être à même de le démontrer si nécessaire (en cas de contrôle par exemple).

Dorénavant, les entreprises ne doivent plus déposer des déclarations préalablement à leurs traitements. Cette formalité dont beaucoup s'interrogeait sur la réelle utilité est supprimée (comparez le nombre d'entreprises en Belgique et le nombre de déclarations introduites auprès de la Commission de la protection de la vie privée et vous comprendrez). Par contre, les sociétés devront pouvoir démontrer à tout moment le fait qu'elles respectent les règles du RGPD. Pour ce faire, l'application d'un code de conduite ou de mécanismes de certification peut aider à démontrer ce principe d'*accountability*.

Selon ce principe de responsabilité, les sociétés doivent avoir une approche responsable, proactive, systématique et continue concernant la protection des données. Les entreprises devront à tout instant pouvoir démontrer qu'elles respectent leurs obligations réglementaires en la matière et ce au travers de l'implémentation de procédures, de mesures et de politiques internes appropriées qui doivent garantir à tout instant l'effectivité et le respect de la protection des données personnelles.

Les mesures ne seront donc pas les mêmes pour toutes les organisations. La politique de protection des données personnelles adoptée au sein d'un organisme devra être définie en fonction de sa taille, de son secteur d'activité, de son personnel, de ses sous-traitants, etc.

B. Mise en œuvre

C'est à ce titre aussi que les sociétés devront dorénavant bien documenter et archiver la moindre de leur décision en la matière afin de pouvoir répondre à une éventuelle question d'une autorité de contrôle des données personnelles ou d'une personne concernée.

La responsabilisation des sociétés, autrement dit le fait qu'elles doivent être continuellement capable de démontrer leur conformité au RGPD (et aux autres règles juridiques bien sûr), ne peut se réaliser d'une manière uniforme mais sur une approche basée sur une analyse des risques qu'elles sont prêtes à prendre.

Ce principe dit de « *risk-based approach* » (qui n'est guère explicité dans le RGPD) est un principe dynamique et global pour l'entreprise : non seulement, la société doit respecter les règles du RGPD mais elle se doit de pouvoir le démontrer à tout instant.

L'analyse d'impact relative à la protection des données (l'AIPD) est un instrument important de ce principe. Il contribue en effet tant au respect des règles qu'à la démonstration de ce respect.

Les mesures techniques et organisationnelles mises en place par le responsable de traitement seront de nature diverse.

Résumons ici les principales obligations qui découlent du principe d'*accountability* :

1. établissement de règles internes assurant sa conformité au RGPD ;
2. établissement d'un registre reprenant l'ensemble des traitements que la société réalise ;
3. réaliser quand cela est nécessaire une AIPD ;
4. veiller au respect des principes de *privacy by design* et de *privacy by default*.

   La protection des données personnelles devra être intégrée dès la conception des systèmes et des technologies mis en place. Le Règlement précise que ce principe devra être décliné tant en phase de détermination des moyens du traitement qu'au moment de sa mise en œuvre ;
5. nommer, si c'est obligatoire, un délégué à la protection des données (un DPD) ;

6. mettre en place la sécurité adéquate autour des données à caractère personnel que la société possède ;
7. veiller à la notification en temps opportun des éventuelles violations de données personnelles.

Comme pour les principes généraux de l'article 5.1 du RGPD, le principe d'*accountability* traverse le Règlement. Il sert de fondement à l'ensemble des principes et exigences qui gouvernent la matière de la protection de nos données personnelles.

C. Les Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail « Article 29 » a adopté des Lignes directrices en rapport avec l'obligation de transparence du responsable du traitement (disponibles uniquement en anglais pour l'instant sur le site internet du Groupe de Travail) (« *Guidelines on transparency under Regulation* 2016/679 », Réf. WP 260).

Ces Lignes directrices sont soumises à consultation jusqu'au 23 janvier 2018. La version finale sera publiée par après.

Fiche de guidance n° 5
Privacy by design et *Privacy by default*

Article 25 du RGPD

Considérant 78 du RGPD

A. Introduction

Le responsable du traitement est également tenu de mettre en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement, des mesures permettant le respect du Règlement (*privacy by design*). Le responsable du traitement devra aussi adopter des mesures permettant de garantir, par défaut, que le traitement est limité à ce qui est nécessaire (*privacy by default*).

Ces notions ne sont pas récentes et vont bien au-delà de la sécurité informatique.

Elles proviennent de travaux canadiens qui datent de 2010. La formulation de l'article 25 du RGPD est toutefois moins ambitieuse que le concept canadien d'Ann Cavoukian, Commissaire à l'information et à la protection de la vie privée de l'Ontario.

B. Implémentation dans le RGPD

1. La *privacy by design*

Selon le texte du RGPD (art. 25.1 du RGPD), le responsable du traitement devra :

mettre en œuvre,

1. tant au moment de la détermination des moyens du traitement

2. qu'au moment du traitement lui-même,

des mesures

1. techniques et
2. organisationnelles appropriées,

a) telles que la pseudonymisation (qui devrait intervenir dès que possible)
b) la minimisation des données

qui sont destinées à mettre en œuvre les principes relatifs à la protection des données.

Les mesures devront :

1. tenir compte de l'état des connaissances,
2. des coûts de leur mise en œuvre et
3. de la nature, de la portée, du contexte et des finalités du traitement
4. ainsi que des risques (dont le degré de probabilité et de gravité varie) que présente le traitement pour les droits et libertés des personnes physiques.

On le voit, après avoir obligé le responsable du traitement à prendre des mesures pour protéger les données personnelles qu'il collecte, le RGPD adoucit l'obligation en précisant que ces mesures peuvent dépendre de leur coût de mise en œuvre, du contexte, des risques du traitement…

Toujours ce jeu d'équilibriste que l'on retrouve dans la plupart des dispositions clef du RGPD.

La pseudonymisation des données permet de ne plus pouvoir associer des données à caractère personnel à une personne physique précise sans avoir recours à des informations supplémentaires. Il s'agit d'une mesure technique et organisationnelle prévue par l'article 32 du RGPD pour garantir la sécurité. Il est conseillé de stocker ces informations supplémentaires séparément des données pseudonymisées.

Le principe de la minimisation des données par défaut vient en complément des principes de la *privacy by design*. La minimisation des données (prévue par l'article 5 du RGPD) consiste à ne traiter que des données adéquates, pertinentes et limitées à la finalité du traitement.

Les mesures choisies par le responsable de traitement pour garantir que seules les données nécessaires au regard de la finalité poursuivie aient été collectées et que le plus haut niveau de protection possible entoure les données personnelles devront être mises en œuvre de façon effective sous le contrôle du Délégué à la Protection des Données (DPD). Cela ne doit pas rester purement théorique.

Le responsable de traitement devra assortir le traitement des garanties nécessaires afin de :

1. répondre aux exigences du RGPD et
2. de protéger les droits de la personne concernée.

Les règles en matière de transparence et de contrôle ainsi que celle en matière de sécurité des données visent aussi à atteindre ces objectifs.

Il est fortement recommandé de formaliser un cahier des charges traduisant les contraintes juridiques en matière de protection des données à caractère personnel (minimisation des données pouvant être traitées, durées proportionnées de conservation des données, limitation des personnes pouvant y accéder, etc.), en contraintes techniques devant être respectées, et qui serait impératif pour tout nouveau projet de programme informatique, de logiciel, d'application.

2. La *privacy by default*

Le responsable du traitement devra, en tenant bien sûr informé son DPD, mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, *par défaut*, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement et donc de leur utilisation, à leur durée de conservation et à leur accessibilité.

Les mesures devront garantir que, *par défaut*, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

Un mécanisme de certification approuvé peut servir d'élément pour démontrer le respect de la *privacy by design* et de la *privacy by default*. Un tel mécanisme n'existe pas encore. Il est étudié au niveau européen.

C. Objectifs

À compter du 25 mai 2018, la dimension de protection des données à caractère personnel devra être intégrée dès la conception d'un projet informatique. En effet, les responsables de traitement devront adopter des mesures qui répondent aux principes de la protection des données par défaut et ce, dès la définition des moyens de traitement des données. Il sera nécessaire de modifier le « *Product Approval Process* » pour les sociétés qui en disposent.

Cette exigence rend aussi indispensable de traiter de la sécurité informatique également dans les contrats avec les sous-traitants notamment par des annexes « Plan d'assurance sécurité » (PAS) ou « *Data breach Process* » (DBP).

Le responsable du traitement et le sous-traitant ont une obligation de moyens renforcé en matière de sécurité au regard de l'état des connaissances. En pratique, l'obligation de protection des données nécessite la mise en œuvre des actions prévues par l'article 32 du RGPD, notamment :

1. la réalisation d'une analyse de risque au regard de la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé accidentel ou illicite aux données ;

2. le choix des mesures techniques adaptées aux risques identifiés (chiffrement, pseudonymisation) ;
3. le contrôle de la qualité des solutions choisies.

Le considérant 78 du RGPD conseille que :

> « lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données ».

La protection dès la conception (*privacy by design*) devrait aussi améliorer le « *return on investment* » (le ROI) de l'organisation et la minimisation des données des consommateurs réduire les coûts marketing et les coûts de stockage.

Le « *privacy by design* » n'est pas simplement dirigé vers les développeurs mais aussi vers les juristes et vers les législateurs quand ils écrivent les lois qui se doivent d'être compréhensibles pour tous.

Notons que faire une bonne AIPD permet aussi d'atteindre les objectifs voulus par le *privacy by design*.

Le *privacy by design* renvoi vers les objectifs que le responsable du traitement veut atteindre et le *privacy by default* est plus sur le comment. Il s'agit d'actions positives que le responsable du traitement doit prendre. Toutes ses actions doivent atteindre les principes généraux de l'article 5 du RGPD.

Toutefois, il n'est pas simple de savoir dans le RGPD comment implémenter ces principes.

La doctrine et les chercheurs en *privacy* et en *data protection* travaillent actuellement sur la mise au point d'outils pour donner des guidances pratiques aux responsables de traitements ainsi que sur le développement de « *Privacy-Enhancing Technologies* » (PET).

Les PET sont des technologies informatiques qui, par défaut, protègent les données à caractère personnel en éliminant les données inutiles ou en ne collectant que les données nécessaires aux traitements envisagés sans que le système qui est derrière perde en fonctionnalité.

Les deux principes présentés ici doivent être pensés dès la construction du traitement mais aussi lors de son exécution. C'est la plus grande difficulté car on touche à deux moments forcément différents.

Un autre questionnement intéressant concerne le champ d'application de ces deux principes. En effet, lorsque l'on conçoit le *privacy by default* et lorsque l'on veille à implémenter les outils qui y sont liés, faut-il aller au-delà du RGPD ? Par exemple, faut-il veiller à protéger uniquement les droits « *privacy* » des personnes concernées ou bien faut-il aller au-delà ?

Fiche de guidance n° 6
Le consentement

Articles 6.1.a, 7 & 9 & 10 du RGPD

Considérants 32, 33, 35, 40 à 49, 51 à 55 & 75 du RGPD

A. Introduction

Le consentement est l'une des six bases juridiques permettant à une société de réaliser un traitement de données à caractère personnel.

Les six bases juridiques sont mentionnées à l'article 6 du RGPD (ce sont à peu près les mêmes que celles qui existent dans la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données).

Un traitement ne sera licite que si :

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère

personnel, notamment lorsque la personne concernée est un enfant. Les autorités publiques dans l'exécution de leurs missions ne peuvent se prévaloir de cette base juridique.

Selon le RGPD (art. 4.11), le consentement de la personne concernée est « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

B. Caractéristiques et conditions du consentement

Les exigences par rapport au consentement ont été renforcées par rapport à la directive de 1995.

Toutefois, le RGPD a introduit des exceptions à la nouvelle définition de consentement. Ce mécanisme fragilise la protection que le texte octroie aux personnes concernées.

En effet, quand on voit la facilité avec laquelle les services numériques obtiennent les consentements de leurs utilisateurs sans que ces derniers ne lisent les informations « *privacy* » de ces sites, il est raisonnable de se demander s'il ne fallait pas restreindre ces possibilités d'exceptions aux règles protectrices du consentement. Est-ce toujours sensé de laisser les conditions de notre protection entre nos mains pour, par exemple, permettre le traitement de nos données de santé ou des transferts hors UE ? Dans le cas où la société entend transférer les données à caractère personnel d'une personne concernée en-dehors de l'UE, elle doit en avoir une base juridique adéquate. Le consentement peut être une de ces bases juridiques.

Pour être correct et valable, le consentement doit être :

1. Libre

   La personne concernée doit disposer d'une véritable liberté de choix : elle doit être en mesure de refuser ou de retirer son consentement sans subir de préjudice. Le consentement est présumé ne pas avoir été donné librement si le consentement doit être donné en une fois pour différentes opérations de traitement des données à caractère personnel ayant des finalités différentes. Dans cette hypothèse, plusieurs consentements doivent être donnés séparément.

   Important : il ne faut pas qu'il existe un déséquilibre manifeste (par exemple hiérarchique ou face à une autorité publique – considérant 43 du RGPD), entre la personne concernée et le responsable de traitement. La personne concernée ne doit véritablement subir aucune pression même purement commerciale (des coûts en plus si le consentement n'est pas donné) lorsqu'elle est amenée à choisir entre donner

ou ne pas donner son consentement à la collecte de données qui la concerne ;

2. Spécifique

   Le consentement peut être demandé pour plusieurs opérations à la fois si ces différentes opérations ont comme objectif la même finalité. *A contrario*, si un responsable du traitement désire traiter les données collectées sur la base d'un consentement pour une autre finalité, il devra redemander le consentement aux personnes concernées ;

3. Éclairée

   Avant de donner son consentement, la personne concernée doit être correctement informée sur, au moins, l'identité du responsable du traitement et les finalités dudit traitement, les catégories de données collectées, l'existence du droit de pouvoir retirer son consentement, sur l'utilisation des données pour créer des décisions fondées uniquement sur des traitements automatiques. De plus, si le consentement est en rapport avec des transferts hors EU, il est nécessaire de fournir à la personne concernée des informations sur les risques en cas de transferts vers des pays qui ne bénéficient pas d'une décision d'adéquation ;

4. Univoque

   Il ne faut pas qu'il y ait de doute sur le choix de la personne concernée ;

5. Donné préalablement à toute collecte ou traitement envisagé.

   Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement doit être présentée sous une forme qui la distingue expressément de ces autres questions et toujours sous une forme compréhensible et aisément accessible, formulée en des termes clairs et simples.

Dans le cas où l'exécution d'un contrat (de travail par exemple) est subordonnée au consentement à des traitements de données à caractère personnel qui ne sont pas nécessaires à l'exécution dudit contrat, il est plus que probable que l'on pourrait considérer que le consentement n'a pas été donné librement dans ce cas. Il s'agit ici d'empêcher l'obtention d'un consentement à un traitement caché dans les termes et conditions d'un contrat, traitement qui ne serait pas en soi strictement nécessaire au contrat en question.

Le responsable du traitement ne peut traiter grâce au contrat (une des six bases juridiques de l'article 6 du RGPD) que les données qui sont strictement nécessaires pour l'exécution du contrat. Obtenir l'accord de la personne concernée pour des finalités de traitement qui sortent du pur champ d'application du contrat est à déconseiller. Le consentement de la personne en effet n'aurait pas été donné librement car il aurait été lié/conditionné à la signature du contrat avec le responsable du traitement.

Exemple

Une banque demande le consentement de ses clients dans le but de traiter les détails de leurs paiements à des fins de marketing. Cette activité de traitement n'est pas nécessaire à l'exécution du contrat qui lie la banque à ses clients. Dans le cas où le refus de consentir par un client aurait comme conséquence la fermeture de son compte, le refus de bénéficier de certains services de la part de la banque ou à une augmentation des frais bancaires qu'il doit payer à la banque, nous pouvons considérer que le consentement comme base juridique n'est pas valable car il n'est pas donné librement.

Principe fondamental s'il en est : la personne concernée a le droit de retirer son consentement à tout moment. Que le responsable de traitement soit rassuré, ce retrait du consentement ne compromettra pas la licéité du traitement fondé sur le consentement effectué avant ce retrait.

La personne concernée doit être informée de la possibilité de retirer son consentement à tout moment avant de donner son consentement (généralement, ce sera le cas via la clause vie privée lisible sur le site internet de la société). Il doit être aussi simple de retirer que de donner son consentement.

C'est ce dernier point qui fait que, même s'il semble à première vue que le consentement soit la base juridique la plus facile à obtenir, nous conseillons aux sociétés d'analyser d'abord s'il n'est pas possible de réaliser le traitement sur la base d'une autre base juridique de l'article 6 du RGPD avant d'opter pour le consentement.

En effet, un consentement (qu'il soit explicite ou non) est précaire car il peut être retiré à tout moment.

Le silence, l'inactivité ou une case cochée par défaut ne peut pas être considéré comme un consentement valable au sens du RGPD puisque le consentement suppose une démarche positive de la part de la personne concernée.

Un responsable du traitement doit toujours s'assurer qu'une personne concernée a donné son consentement après avoir pu facilement identifier qui est le responsable du traitement et quelles seront les conséquences de son consentement. Il est du devoir (cela découle du principe de transparence) du responsable du traitement de bien décrire les finalités poursuivies par ses activités de traitement pour lesquelles il requiert le consentement des personnes concernées. L'écriture de cette description dépendra du public cible.

C. Le consentement explicite

Le responsable du traitement devra obtenir un consentement explicite de la part de la personne concernée dans certaines situations plus à risque pour la protection des données à caractère personnel :

1. pour les traitements des données énumérées à l'article 9 du RGPD ;
2. lorsque les données personnelles vont être transférées hors de l'Union européenne vers des pays ou organisations internationales en cas d'absence de garanties adéquates (article 49.1.a du RGPD) ;

3. en cas de décisions purement automatiques en vertu de l'article 22 du RGPD.

La personne concernée devra expressément exprimer son consentement à de tels traitements par exemple, par le biais de sa signature écrite (et scannée dans le cas d'une procédure électronique).

1. Traitement des données « particulières » de l'article 9 du RGPD

Dans le cas où une société entend traiter des données particulières au sens de l'article 9 du RGPD (données médicales par exemple), elle doit aussi en avoir la base juridique adéquate. Le consentement explicite peut être une de ces bases juridiques sauf si le droit de l'Union ou le droit de l'État membre prévoit qu'il n'est pas possible de traiter ces données spéciales sur la base de ce consentement explicite.

La Directive de 1995 protégeait déjà ces données spéciales ou sensibles mais le RGPD a élargi cette catégorie de données.

Les données « particulières » sont les données à caractère personnel qui révèlent :

- l'origine raciale ;
- l'origine ethnique ;
- les opinions politiques ;
- les convictions religieuses ;
- les convictions philosophiques ;
- l'appartenance syndicale.

Ce sont aussi :

- les données génétiques ;
- les données biométriques qui permettent d'identifier une personne physique de manière unique ;
- les données concernant la santé ;
- les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Les traitements des données de l'article 9 du RGPD sont aussi permis sous d'autres conditions (article 9.2.b à 9.2.j du RGPD).

Certaines des exceptions à l'interdiction de principe de traiter ces catégories de données personnelles étaient déjà prévues par la Directive de 1995 mais elles sont bien plus nombreuses sous l'empire du RGPD. La protection des personnes concernées en est d'autant plus réduite.

De plus, les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la

santé. Dès lors, non seulement, la protection des personnes concernées est ici réduite mais, en outre, la marge de manœuvre ainsi laissée aux États membres créera une incertitude juridique du fait de la disparité normative qu'elle crée.

Nous retrouvons cette problématique du « j'octrois des droits aux personnes concernées que je compense par des facilités offertes (directement ou indirectement) aux responsables du traitement » plusieurs fois dans le RGPD. Il s'agit d'un texte ambitieux mais n'oublions pas qu'il s'agit d'un texte législatif issu de (très !) nombreux compromis.

2. Décision individuelle exclusivement automatisée

a. *Règle générale*

Selon l'article 22 du RGPD, la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Toutefois, ce droit n'est pas absolu.

b. *Exceptions*

En effet, la personne ne peut s'opposer à une telle décision purement automatique lorsque la décision en question :

a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;

b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ou

c) est fondée sur le consentement explicite de la personne concernée.

c. *En cas d'application d'une des trois exceptions*

Dans les cas visés aux points a) et c) ci-dessus (contrat et consentement explicite), le responsable du traitement devra mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée. La personne concernée devra pouvoir au moins :

1. obtenir une intervention humaine de la part du responsable du traitement,
2. exprimer son point de vue et
3. contester la décision.

D. Conditions applicables au consentement des enfants en ce qui concerne les services informatiques

Le consentement d'un enfant n'est licite que si l'enfant est âgé d'au moins 16 ans.

Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.

Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans. À voir donc si la Belgique va activer cette option ou pas. Plusieurs pays comme la Grande-Bretagne ou l'Irlande ont décidé d'ores et déjà d'activer l'option pour descendre la limite d'âge à 13 ans tandis que l'Espagne gardera sa limite actuelle de 14 ans.

Le responsable du traitement devra s'efforcer de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles. Le projet de règlement dit en quelque sorte que la charge de la preuve du consentement va incomber aux responsables du traitement de l'information. Les États vont donc se décharger complètement du mode de contrôle en disant aux entreprises du web qu'il leur appartiendra de démontrer qu'elles ont eu le consentement explicite.

En pratique : les professionnels devront redoubler de vigilance pour ce public

- Rédiger le formulaire de collecte de données en termes clairs et simples « que l'enfant peut aisément comprendre ». En pratique, l'on recommandera par exemple d'utiliser le tutoiement dans un formulaire de collecte de données français destiné à des enfants.
- S'assurer que le titulaire de l'autorité parentale est bien à l'origine du consentement lié au recueil des données de l'enfant. Les responsables de traitement devront procéder à cette vérification « compte tenu des moyens technologiques disponibles ». Concrètement, cela implique de mettre en place des mécanismes de contrôle, par exemple des messages d'avertissements mentionnant les sanctions applicables en cas de fausse déclaration.
- Permettre aux enfants devenus majeurs de retirer leur consentement.

E. Droit à l'effacement (« droit à l'oubli »)

Selon l'article 17 du RGPD, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque la personne concernée retire le consentement sur lequel est fondé le traitement

(conformément à l'article 6.1.a ou à l'article 9.2.a) et s'il n'existe pas d'autre fondement juridique au traitement.

Autrement dit, la personne concernée pourra faire jouer son droit à l'effacement de ses données dans le cas où :

1. le responsable du traitement a obtenu les données personnelles sur la base juridique du « consentement » ;
2. la personne concernée retire son consentement sur lequel est fondé le traitement (autrement dit, pas d'effacement possible si pas de retrait en même temps) ;
3. il n'existe pas d'autre fondement juridique au traitement.

Le responsable du traitement devra refuser l'effacement exigé dans la mesure où ce traitement est nécessaire :

a) à l'exercice du droit à la liberté d'expression et d'information ;
b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9.2.h et 9.2.i ainsi qu'à l'article 9.3 du RGPD ;
d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89.1, dans la mesure où le droit est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ou
e) à la constatation, à l'exercice ou à la défense de droits en justice.

F. Lien avec le droit à la portabilité des données

Suite à l'article 20 du RGPD, les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque (deux conditions cumulatives) :

a) le traitement est fondé sur le consentement en application de l'article 6.1.a ou de l'article 9.2.a ou sur un contrat en application de l'article 6.1.b du RGPD et
b) le traitement est effectué à l'aide de procédés automatisés.

La personne concernée a aussi le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.

G. Le registre des consentements

Selon l'article 7 du RGPD, dans les cas où le traitement repose sur le consentement, le « responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant ».

La charge de la preuve en cas de contestation repose sur les épaules du responsable du traitement. Il devra donc garder que ce soit dans son registre des traitements ou dans un registre séparé, une trace que le traitement en question repose bien sur le consentement (voire sur le consentement explicite) de la personne concernée.

H. Les Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail « Article 29 » a adopté, le 28 novembre 2017, des Lignes directrices en rapport avec le consentement (disponibles uniquement en anglais pour l'instant sur le site du Groupe de Travail) (« *Guidelines on Consent under Regulation* 2016/679 », Réf. WP 259).

Ces Lignes directrices sont soumises à consultation jusqu'au 23 janvier 2018. La version finale sera publiée par après.

Ces Lignes directrices de 2017 viennent compléter un document émis le 13 juillet 2011 sur le consentement (« Avis 15/2011 sur la définition du consentement », Réf. WP 187).

I. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 23 : Droit 6 : Le droit à la portabilité des données*
- *Fiche de guidance n° 25 : Droit 8 : Le droit à ne pas faire l'objet d'une décision automatique, y compris le profilage*

Fiche de guidance n° 7
Les intérêts légitimes

Article 6.1.f du RGPD

Considérants 40 à 49 du RGPD

A. Introduction

Nous l'avons mentionné dans la Fiche de guidance n° 6 consacrée au consentement, un traitement ne sera licite que s'il repose sur une des six bases juridiques de l'article 6.1 du RGPD.

Une des bases juridiques la moins évidente à comprendre est celle relative aux « intérêts légitimes » du responsable du traitement. Cette base juridique existait déjà sous l'empire de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données en son article 7.f.

B. Analyse

Selon l'article 6.1.f, le traitement peut être licite si, et dans la mesure où, il est :

> « nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. »

Cette base juridique ne peut s'appliquer à des traitements effectués par les autorités publiques dans l'exécution de leurs missions.

Fonder un traitement de données sur cette base juridique n'est pas si facile.

En effet, il impliquera toujours, pour le responsable de traitement, de faire préalablement à son activité de traitement une analyse systématique de la balance des intérêts en présence.

Le responsable de traitement devra réaliser ce que l'on peut appeler un « *Legitimate Interest Assessment* » (un « LIA »).

C. Présentation du LIA

Ce LIA comportera trois étapes :

1. l'identification des intérêts légitimes du responsable ou d'un tiers à qui les données seront communiquées à la réalisation dudit traitement (les intérêts devront être réels et pas spéculatifs) : quelle est la finalité du traitement et pourquoi ce traitement est-il important pour le responsable ou un tiers ? Même si ces intérêts paraissent évidents, il faudra les communiquer clairement aux personnes concernées ainsi que la possibilité de s'y opposer ;
2. la détermination de la nécessité pour le responsable de traitement à réaliser ledit traitement.

   Le responsable de traitement doit analyser en quoi la réalisation de ce traitement est nécessaire à la poursuite de ses objectifs commerciaux. Afin de savoir si un traitement est nécessaire, le responsable du traitement devra se poser la question suivante : y a-t-il un autre moyen de parvenir aux intérêts identifiés ?

   a) si la réponse est négative, clairement, le traitement est nécessaire ;

   b) si un autre moyen est possible mais requiert des efforts disproportionnés, le traitement est aussi nécessaire ;

   c) si plusieurs moyens équivalents sont possibles, il est alors indispensable de réaliser une AIPD afin d'identifier la manière la moins intrusive de parvenir aux intérêts identifiés ;

   d) si le traitement n'est pas nécessaire, dans ce cas, le responsable ne peut se baser sur ce fondement juridique pour réaliser son traitement ;

3. la mise en balance des intérêts ou des libertés et droits fondamentaux de la personne concernée par le traitement par rapport aux intérêts légitimes du responsable de traitement à réaliser ledit traitement.

   Cette analyse devra se réaliser équitablement en tenant compte de tous les droits et libertés de la personne concernée, de la nature des intérêts identifiés, des données concernées par le traitement, de l'impact du

traitement ainsi que des mesures que le responsable a mis en place afin de diminuer les impacts potentiellement négatifs.

Dans le cas où les intérêts ou les droits et libertés de la personne concernée exigeant une protection des données à caractère personnel sont supérieurs aux intérêts légitimes du responsable à réaliser le traitement, ils empêchent la réalisation du traitement concerné.

Il doit exister un réel lien entre le traitement et l'intérêt poursuivi afin de garantir que le traitement des données fondé sur l'intérêt légitime ne débouche pas sur une interprétation trop large de la nécessité de traiter les données. Il y aura toujours lieu d'examiner s'il n'existe pas d'autres moyens plus respectueux de la vie privée susceptibles de servir la même finalité.

Nous vous conseillons surtout de toujours documenter l'analyse réalisée.

Rappelons que s'il fallait retenir un seul mot du RGPD, c'est le mot « documentation » qui doit venir à l'esprit. Nous conseillons en effet de toujours tout documenter et archiver afin de pallier toute question future d'une personne concernée ou de l'autorité.

D. Présentation d'une analyse en étapes

Il est possible aussi de déterminer si votre traitement peut se baser sur cette base juridique selon une autre méthode. Nous vous la présentons ci-après.

Il s'agit d'une analyse en étapes. La société devra se poser une série de questions. Si, à un moment, elle se doit de répondre par la négative, la possibilité de se baser sur les intérêts légitimes n'est pas possible pour elle pour le traitement concerné. Cela ne veut pas dire que le traitement est en soi illicite mais que la société devra en rechercher une autre base juridique.

1. Est-ce que toutes les autres bases juridiques ont-elles été analysées ? (*pertinence*)
2. La finalité poursuivie par la société est-elle légitime ? (*licéité*)
3. L'intérêt poursuivi par la société par la finalité est-il réel et actuel ? (*réalité*)
4. Le traitement voulu est-il indispensable à la finalité poursuivie ? (*nécessité et proportionnalité*)
5. Avez-vous identifié les droits et intérêts des personnes concernées ainsi que leurs attentes raisonnables ?
6. Ces droits, intérêts ou attentes entrent-ils en conflit avec votre intérêt légitime ?
7. Si tel est le cas, pouvez-vous analyser et déterminer que vos intérêts légitimes prévalent sur ces droits, intérêts et attentes ?
8. Avez-vous implémenté des mesures pour protéger raisonnablement les droits des personnes concernées ?
9. Avez-vous garder suffisamment de documentation dans le but de pouvoir démontrer votre « *accountability* » et votre « *compliance* » au RGPD ?
10. Avez-vous prévu des procédures pour permettre aux personnes concernées de s'opposer à un tel traitement ?

E. Exemples

Peuvent constituer un intérêt légitime du responsable du traitement concerné (il est évident qu'il existe bien d'autres exemples qui vont dépendre des activités de chaque responsable du traitement) :

1. la défense contre les attaques cybernétiques.

   L'exploitant d'un site Internet peut avoir un intérêt légitime à conserver certaines données à caractère personnel des visiteurs afin de se défendre contre les attaques cybernétiques (arrêt de la CJUE dans l'affaire C-582/14 *Patrick Breyer/Bundesrepublik Deutschland* du 19 octobre 2016) ;

2. les traitements strictement nécessaires à des fins de prévention de la fraude (considérant 47 du RGPD) ;

3. les traitements à des fins de prospection/marketing direct (considérant 47 du RGPD) ;

4. les transmissions de données à caractère personnel au sein d'un groupe de sociétés à des fins administratives internes (considérant 48 du RGPD) ;

5. les traitements de données à caractère personnel dans la mesure strictement nécessaire et proportionnée aux fins de garantir (considérant 49 du RGPD) :

   a) la sécurité du réseau et des informations (autrement dit la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées ou transmises),

   b) la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, par des autorités publiques, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes d'intervention en cas d'incidents de sécurité informatique (CSIRT), des fournisseurs de réseaux et de services de communications électroniques et des fournisseurs de technologies et services de sécurité.

   Il pourrait s'agir, par exemple, d'empêcher l'accès non autorisé à des réseaux de communications électroniques et la distribution de codes malveillants, et de faire cesser des attaques par « déni de service » et des dommages touchant les systèmes de communications informatiques et électroniques.

Fiche de guidance n° 8
Le registre des traitements

Article 30 du RGPD

Considérant 82 du RGPD

A. Principe

Lorsque le RGPD sera en vigueur, les sociétés ne devront plus déclarer leurs traitements aux autorités de contrôle nationales.

Cette obligation a été en quelque sorte internalisée. En effet, selon l'article 30 du RGPD, chaque responsable de traitement et chaque sous-traitant devra tenir un registre des activités de traitement effectuées sous leur responsabilité. Ce registre fait partie de l'*accountability* de chaque organisation qui réalise des traitements. En effet, cette cartographie en mode continu de ses activités doit permettre à toute société de bien veiller à toujours respecter les règles du RGPD.

Les registres devront être mis à la disposition de l'autorité de contrôle des données personnelles en cas de demande de celle-ci. Le registre n'est pas destiné au public.

Le RGPD précise que ces registres peuvent se présenter sous une forme écrite y compris la forme électronique. Ils ne devront pas être spécialement réalisés dans une des trois langues nationales. Toutefois, lors de la mise à disposition à une autorité de contrôle des données personnelles, celle-ci pourrait exiger sa traduction dans une des langues nationales.

La tenue de ce registre est nécessaire pour les responsables pour avoir une connaissance suffisamment documentée de leurs activités de traitement des données et donc pour en assurer une protection efficace.

B. Contenu du registre

1. Le registre du responsable du traitement

Quelques illustrations de traitements habituels de données à caractère personnel

Gestion du personnel et des rémunérations, annuaire d'entreprise, gestion des fournisseurs, gestion de la comptabilité, gestion des clients et des opérations commerciales, de fidélisation et de prospection, gestion des outils informatiques, lutte contre la fraude (interne/externe), surveillance (vidéo, alarme, contrôle des accès, …).

Le registre du responsable du traitement (ou de son représentant le cas échéant) devra contenir un certain nombre d'informations dont au moins (libre à la société d'aller au-delà) :

1. des données d'identification comme le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
2. les finalités de chaque traitement ;
3. pour chaque traitement, une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
4. les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
5. le cas échéant, l'identification des transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris la mention de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49.1, deuxième alinéa du RGPD, les documents attestant de l'existence de garanties appropriées ;
6. dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
7. également dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32.1 du RGPD.

Le Registre devra, à partir du 25 mai 2018, contenir les éléments d'informations détaillés ci-dessus au regard des traitements opérés à la date du 25 mai 2018, qu'ils soient opérés de longue date ou plus récemment.

L'autorité de contrôle des données personnelles belge a précisé que, au regard des traitements de données, un certain nombre d'informations supplémentaires seront exigées.

Le Registre des activités de traitement est, comme son nom l'indique, un Registre de traitements et non pas un Registre contenant les données traitées. La nuance est d'importance.

L'obligation de tenir un Registre des traitements est une obligation dynamique, en ce sens que le responsable de traitement et le sous-traitant devront veiller à le tenir à jour en ajoutant, par exemple, tout nouveau destinataire qu'ils n'auraient pas pu envisager lors de la rédaction originelle du Registre (ex : inspection fiscale, nouveau partenaire commercial).

Quant au délai de conservation des informations contenues dans le Registre une fois que le traitement a cessé, le RGPD ne précise rien. De l'avis de l'autorité de contrôle des données personnelles belge, il peut être utile pour les responsables de traitement et les sous-traitants de conserver cette information – avec mention de ce que le traitement a été opéré de telle à telle date par exemple – à des fins d'*accountability*. En effet, l'autorité de contrôle est susceptible de demander accès à ce Registre dans le cadre de contrôles qu'elle peut mener (après la cessation du traitement) dans le respect des délais de prescription des actions qui lui seront applicables.

Rien ne s'oppose à ce que le Registre contienne davantage d'informations. Toutefois, les sociétés ne doivent pas oublier que ces éléments devront, le cas échéant, être communiqués à l'autorité de contrôle à première demande.

2. Le registre du sous-traitant

Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant, tiendra aussi un registre. Ce registre devra reprendre toutes les catégories d'activités de traitement effectuées pour chaque responsable du traitement. Il y aura donc autant de registres qu'il y aura de responsable de traitement avec qui le sous-traitant travaille.

Chaque registre devra comprendre au moins :

1. des données d'identification comme le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles de son délégué à la protection des données ;
2. les catégories de traitements effectués pour le compte de chaque responsable du traitement ;
3. le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49.1, deuxième alinéa du RGPD, les documents attestant de l'existence de garanties appropriées ;
4. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32.1 du RGPD.

On le voit, il s'agit des mêmes informations que celles devant figurer dans le registre du responsable du traitement à l'exception notable de l'indication des délais prévus pour l'effacement des différentes catégories de données puisque la politique d'effacement sera décidée par le responsable du traitement à chaque fois.

C. Exemption

Il est possible pour les petites sociétés de ne pas devoir tenir un tel registre. Toutefois, cette possibilité est très limitée.

En effet, seront exemptées uniquement les organisations qui comptent moins de 250 employés et qui :

a) ne réalisent pas de traitements qui sont susceptibles de comporter un risque pour les droits et des libertés des personnes concernées ou

b) réalisent des traitements qui sont purement occasionnels (dès lors une PME qui réalise des traitement courants (= qui ne sont pas occasionnels) devra tenir un registre indépendamment du risque que pourrait occasionner lesdits traitements) ou

c) ne réalisent pas de traitements qui portent notamment sur les catégories particulières de données visées à l'article 9.1 du RGPD (des données de santé par exemple) ou

d) ne réalisent pas de traitements qui portent sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 du RGPD.

Les cas pour bénéficier de l'exemption de tenir un registre seront peu fréquents. Car dès qu'une société voudra envoyer régulièrement une newsletter ou réaliser du direct marketing, elle devra tenir un tel registre.

Dans les cas où l'exemption s'applique, il apparaît que nous n'aurons plus aucune connaissance de la réalisation des traitements puisque l'obligation de les déclarer à une autorité de contrôle des données personnelles a été abrogée.

Pour finir, retenons aussi qu'il s'agit, à côté de celle relative au Délégué à la Protection des Données, de la seule dérogation « PME » dans le RGPD.

D. Exemples de registre

L'autorité belge de protection des données personnelles a publié, début août 2017, un canevas de registre très étendu (ainsi que des explications sur comment remplir ledit registre). La CNIL française a fait de même sur son site web.

Les modèles, en Excel, sont assez classiques et faciles d'utilisation.

E. Lignes directrices

L'autorité de contrôle des données personnelles belge a publié le 14 juin 2017 une Recommandation relative au Registre des activités de traitements (CO-AR-2017-011).

Le texte est disponible en français et en néerlandais.

Fiche de guidance n° 9
La protection des données personnelles

Article 32 du RGPD

Considérant 83 du RGPD

A. Introduction

La sécurité est sans aucun doute une composante majeure du RGPD. En effet, l'obligation pour le responsable du traitement d'adéquatement sécuriser les données à caractère personnel qu'il a collectées se retrouve en filigrane dans l'ensemble des dispositions applicables et sous-tend l'ensemble des obligations en matière de protection des données à caractère personnel.

Pour garantir la sécurité et prévenir tout traitement effectué en violation du règlement, le responsable du traitement ou le sous-traitant devra évaluer les risques inhérents au traitement visé et mettre en œuvre des mesures pour atténuer les risques, telles que le chiffrement ou un accès aux données à double clef.

Il s'agit ici d'obliger le responsable du traitement et le sous-traitant à mettre en œuvre les mesures appropriées pour assurer la sécurité du traitement et pour garantir un niveau de sécurité approprié au risque.

Le RGPD encourage l'adoption de mécanisme de certification comme un moyen de prouver la conformité de la société.

La conformité avec la norme ISO 27001 « *international information security standard* » (il s'agit du seul standard international et indépendant en matière de sécurité des données) pourrait aider grandement les sociétés à démontrer leur conformité avec les exigences de sécurité du RGPD. Implémenter le standard ISO 27001 implique de construire une approche holistique incluant les traitements, le personnel et les technologies utilisées à travers toute la société dans le but de sécuriser les informations détenues et produites par la société.

Ces mesures doivent assurer un niveau de sécurité approprié, y compris en matière de confidentialité, compte tenu de l'état des connaissances techniques et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger.

Dans le cadre de l'évaluation des risques pour la sécurité des données, le responsable du traitement devra tenir compte des risques que présente vis-à-vis de la personne concernée le traitement de données à caractère personnel qu'il envisage de réaliser.

Ces risques peuvent être la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral à l'égard de la personne concernée.

B. Principe

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant devront mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Si une politique générale de sécurité des systèmes d'information existe habituellement au sein de toute entreprise, il est recommandé de formaliser également une politique de sécurité dédiée cette fois-ci à la protection des données à caractère personnel dans la mesure où les éléments devant y être prévus présentent une certaine spécificité.

Les mesures techniques et organisationnelles appropriées sont entre autres et selon les besoins :

1. la pseudonymisation et le chiffrement des données à caractère personnel. Attention, il est difficile de chiffrer les emails même s'il existe des services de messagerie chiffrée, comme ProtonMail ou Mailpile, où le chiffrement automatique se réalise uniquement entre deux boîtes du même fournisseur ;
2. des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité/accessibilité et la résilience constantes des systèmes et des services de traitement ;
3. des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
4. une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles mises en place pour assurer la sécurité du traitement.

C. Évaluation du niveau de sécurité

Pour évaluer si le niveau de sécurité est approprié, le responsable du traitement devra tenir compte des risques encourus pour les données elles-mêmes, en particulier :

- la destruction,
- la perte,
- l'altération,
- la divulgation non autorisée des données transmises, conservées ou faisant l'objet d'un traitement ou
- l'accès non autorisé aux données de manière accidentelle ou illicite.

L'application d'un code de conduite approuvé comme le prévoit l'article 40 du RGPD ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir comme élément pour démontrer le respect des exigences du Règlement.

Le responsable du traitement et le sous-traitant devront prendre des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

La sécurité est aussi l'affaire de chaque utilisateur. Chaque internaute se doit d'appliquer certaines mesures de sécurité physique et logique classiques – mais encore insuffisamment mises en œuvre.

Peuvent être citées en exemple comme mesures de sécurité :

1. les moyens d'identification et d'authentification qui incluent la définition d'une politique de gestion des mots de passe dynamiques ;
2. la gestion des habilitations de chaque utilisateur et son corollaire indispensable, le contrôle régulier de la traçabilité des accès ;
3. la sécurisation physique et logique des postes de travail (locaux fermés et surveillés, pare-feux, antivirus) et, pour les outils mobiles, chiffrement des données lors de leur transfert vers un système d'information ;
4. l'encadrement des activités de sous-traitance et en particulier de maintenance sur les systèmes ;
5. plans de continuation/de reprise d'activité et/ou plan de secours informatique ainsi que la définition d'une politique de sauvegarde assurant la restitution intègre des données ;
6. l'interdiction d'utilisation des réseaux sociaux sur les lieux de travail et le rappel qu'il faut y publier le moins possible de données personnelles et surtout sensibles. Il faut éviter d'y publier des mots de passe

et des adresses physiques. Rappelons qu'il existe aussi des réseaux sociaux qui précisent dans leurs Conditions Générales d'Utilisation qu'ils ne vont pas utiliser vos données personnelles à des fins de prospection.

Voici aussi quelques bonnes pratiques valables pour tous :

1. établir une charte de bonnes conduites ;
2. former les experts et l'ensemble des acteurs ;
3. identifier les personnes compétentes au sein de sa structure ;
4. procéder régulièrement à des analyses de risques et mettre en place les mesures de prévention nécessaires ;
5. intégrer les différentes mesures de sécurité dans le fonctionnement quotidien des services ;
6. écrire une procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles prises pour la sécurité des traitements.

   Cette procédure doit être réalisée en concertation avec des auditeurs techniques et juridiques. Une telle procédure d'audit de sécurité doit également être déployée auprès des sous-traitants par les responsables de traitement ;
7. réaliser souvent des séances d'informations sur les menaces les plus courantes (le *ransomware*, le *phishing*, les vols de mots de passe, l'accès à des faux sites, l'accès à des réseaux Wi-Fi piégés, etc.) et sur comment les éviter.

   Il faut conseiller d'être très vigilant et d'éviter d'ouvrir des mails ou fichiers inconnus et de communiquer intempestivement des données sensibles ou des données financières via des réseaux inconnus ou sur des sites inconnus ou à la présentation étrange ;
8. etc.

Les données, les systèmes et les processus qui nécessitent une protection particulière doivent être clairement identifiés. Les différents types d'informations qui y circulent nécessitent, en effet, des niveaux de protection adaptés.

L'élément clé de toute démarche en la matière repose sur l'analyse de risques.

Ensuite viendront les choix et la mise en place des mesures de sécurité acceptables pour l'entreprise. Les bonnes personnes doivent être associées à ce genre de décisions. Le traitement des risques cyber doit être réalisé conjointement par les experts sécurité et par les personnes du métier. Une approche rationnelle est nécessaire, la cybersécurité étant l'affaire de tous. Les décideurs doivent s'approprier le sujet, intégrer ces risques et faire circuler leurs décisions.

Il est important de diffuser une culture du risque au sein de chaque entreprise et de mettre en place des outils avec des droits d'accès, du matériel durci dédié…

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) française identifie aujourd'hui quatre grands types de menaces :

1. la déstabilisation, qui s'avère une menace importante, avec un impact souvent critique ;
2. les menaces de type cybercriminalité, avec comme grande tendance le phénomène des *ransomwares* ;
3. l'espionnage, qui repose généralement sur un mode opératoire sophistiqué ;
4. le sabotage, via des outils comme Stuxnet, qui ont un impact souvent colossal.

La société devra se protéger contre toute violation des données tout le long de la durée de vie des données (de leur collecte à leur destruction finale en passant par chacune de leur utilisation). Le RGPD protège en effet les droits des personnes concernées contre toute atteinte non voulue sur les données qu'elles ont (temporairement) confiées à la société en qui elles ont placé leur confiance.

D. La protection des bâtiments : un fondamental à ne pas négliger

La sécurité des locaux est la première des protections à avoir. Les conditions d'accueil et d'accès des personnes extérieures à l'entreprise sont encore mal maîtrisées aujourd'hui, et ces dernières peuvent souvent se balader à leur guise dans les locaux. Laisser les différents acteurs aller et venir dans son entreprise est déjà la première des faiblesses et est potentiellement risqué. S'il s'agit d'un cas d'espionnage par la concurrence ou autre, cela peut avoir comme conséquence la perte de marchés, d'où l'importance de mettre en place les mesures de protection adéquates.

Les entreprises doivent renforcer leur sécurité physique et avoir une véritable politique de sûreté et de protection des bâtiments, afin de prévenir les risques et de lutter contre les modes d'action des malfaiteurs. Les cambriolages font, en effet, partie des risques à ne pas négliger. On parle ici bien entendu des infractions contre les biens, mais aussi contre les personnes (menaces et/ou violence). Les préjudices liés à ce type de méfaits sont souvent très importants. Pour réussir ce type d'acte malveillant, il faut généralement la réunion de trois facteurs : un délinquant motivé, une cible et l'absence de gardien ou de mesures de protection suffisantes.

Pour mieux se défendre, une société n'a d'autre choix que d'obliger un délinquant à accroître ses efforts, mais aussi faire peser sur lui un risque plus important d'être reconnu. Plus le risque d'être détecté ou reconnu est important pour le délinquant, moins il aura de chance de passer à l'acte.

L'entreprise peut également réduire son intérêt en tant que cible et faire en sorte que le risque soit le plus faible possible. Pour ce faire, chaque entreprise peut diminuer les valeurs (argent, œuvres d'art, etc.) qu'elle possède et le faire savoir. Elle se doit aussi d'améliorer ses équipements, ses infrastructures, renforcer son contrôle d'accès et sa protection intérieure, périmétrique et périphérique. Par exemple, les accès arrières sont souvent moins bien protégés que l'entrée principale. Il est essentiel d'avoir un regard extérieur autour de son entreprise et de limiter ainsi les facilitateurs d'intrusions.

Les sociétés ont souvent des faiblesses au niveau des accès, des portes, des serrures… L'ensemble de ces aspects nécessitent une réflexion en amont quant à la stratégie de protection des locaux, au même titre que les données. La protection des bâtiments (contrôle d'accès, coffres, vidéoprotection, signalétique, alarmes, …) doit être fondamentale pour tout chef d'entreprise, d'autant que les conséquences d'un acte malveillant sont souvent dramatiques.

Fiche de guidance n° 10
L'analyse d'impact relative à la protection des données (AIPD)

Article 35 du RGPD

Considérants 72, 84 & 89 à 95 du RGPD

A. Principe

Le RGPD précise que lorsque des traitements considérés comme particulièrement risqués sont envisagés par un responsable, celui-ci devra réaliser, préalablement à ces traitements, une analyse d'impact relative à la protection des données (« AIPD » par après).

Le Groupe de Travail « Article 29 » a publié début octobre 2017 des Lignes directrices très importantes sur le sujet.

Cette étude des risques va conditionner les mesures techniques et organisationnelles que le responsable du traitement va décider de prendre dans le but de protéger les données qu'il a collectées.

B. Réalisation

1. Introduction

Les responsables du traitement ont l'obligation générale de gérer adéquatement les risques liés aux traitements des données à caractère personnel.

Une AIPD est dès lors une analyse visant :

- à évaluer les risques liés aux droits et libertés des personnes concernées qui surviennent ou menacent de survenir dans le cadre du

traitement de données à caractère personnel opéré par le responsable du traitement en question et

- à évaluer les possibilités de gestion de ces risques.

Les deux aspects sont fondamentaux : analyse des risques potentiels et diminution de leur impact.

L'AIPD fait partie du principe de responsabilité (d'*accountability*) par lequel non seulement, les sociétés doivent respecter les règles du RGPD mais se doivent aussi de pouvoir le démontrer à tout instant. Le rapport relatif à une AIPD contribuera tant au respect des règles qu'à la démonstration de leur respect.

Suite à la réalisation d'une AIPD (qui doit donc être réalisé *avant* les opérations de traitement), le responsable sera amené à prendre plus de protection pour les traitements à risque(s) élevé(s) que pour des traitements à risque faible.

Selon l'approche fondée sur le risque du RGPD, la réalisation d'une AIPD n'est pas obligatoire pour chaque opération de traitement. En effet, selon l'article 35 du RGPD, l'obligation pour un responsable du traitement de réaliser une AIPD ne s'applique que pour les traitements « susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

Dès lors, une AIPD n'est pas nécessaire dans les cas suivants :

1. lorsque le traitement n'est pas « susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques » ;
2. lorsque la nature, la portée, le contexte et les objectifs du traitement sont très semblables au traitement pour lequel une AIPD a déjà été effectuée.

   Dans de tels cas, les résultats de l'AIPD pour un traitement similaire peuvent être utilisés ;
3. lorsque les activités de traitement ont été vérifiées par une autorité de contrôle avant mai 2018 pour des situations bien spécifiques qui n'ont pas changé et si les activités de traitement sont exécutées toujours de la même manière à celle qui existait lors ladite vérification ;
4. lorsqu'une opération de traitement a une base juridique dans la législation de l'UE ou d'un État membre, lorsque la loi réglemente l'opération de traitement spécifique et que l'AIPD, selon les normes du RGPD, a déjà été menée dans le cadre de l'établissement de cette base juridique à moins que la loi en question ne précise qu'une AIPD doit quand même être réalisée ;
5. lorsque le traitement est inclus dans la liste facultative (établie par l'autorité de contrôle nationale) des opérations de traitement pour lesquelles aucune AIPD n'est requise. Dans de tels cas, une AIPD n'est pas nécessaire.

Conformément à l'article 70.1.e du RGPD, le futur Comité européen de la protection des données (CEPD) pourra publier des lignes directrices, des recommandations et des bonnes pratiques en matière d'AIPD.

Les autorités de contrôle des données personnelles devront établir et publier une liste des types d'opérations de traitement pour lesquelles une AIPD est obligatoire.

Elles pourront (ce n'est ici qu'une faculté) aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. Les deux listes seront très utiles pour les sociétés actives avec des traitements de données personnelles.

L'autorité de contrôle belge a publié ses listes dans sa recommandation n° 01/2018 du 28 février 2018.

2. Les acteurs concernés

L'obligation de procéder à une AIPD incombe au responsable du traitement pas au DPD en tant que tel.

C'est la société qui sera responsable en vertu de l'article 35 du RGPD si l'AIPD n'a pas été réalisée alors qu'elle aurait dû l'être, si elle n'a pas été correctement réalisée ou si le responsable n'a pas consulté l'autorité de contrôle compétente lorsque c'est nécessaire.

L'amende administrative pourra monter jusqu'à 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires mondial annuel de l'exercice précédent, le montant le plus élevé étant retenu.

Les bonnes personnes au sein de l'entreprise doivent être impliquées en temps utile dans la réalisation de l'AIPD et dans le processus d'appréciation du risque. Il s'agit (e.a.) du DPD (s'il y en a un), du conseiller en sécurité (de nouveau, s'il y en a un), les concepteurs des nouvelles applications ou des nouveaux logiciels, ceux qui prennent les décisions stratégiques en matière de développement de projets, les employés qui utiliseront ces nouveaux outils, le top management, les personnes concernées (ou leurs représentants) par les traitements prévus, l'autorité de contrôle des données personnelles si les risques résiduels restent élevés, etc.

En faire la liste n'est pas si facile et dépendra du cas par cas.

En tout cas, l'appréciation du risque (avec ou sans l'AIPD), l'approbation de l'AIPD ainsi que la décision de ne pas procéder à une AIPD devront être officiellement soumises à l'appréciation et à l'accord des membres de la direction de la société responsable du traitement.

Le sous-traitant devra, en fonction de la nature du traitement, assister le responsable du traitement dans l'exécution de l'AIPD (art. 28.3.f et considérant 95 du RGPD).

3. Contenu d'une AIPD

Une AIPD peut concerner une seule opération de traitement.

Toutefois, l'article 35.1 stipule qu'

« une évaluation unique peut traiter un ensemble d'opérations de traitement similaires présentant des risques élevés similaires ».

Le considérant 92 ajoute qu'

« il existe des circonstances dans lesquelles il peut être raisonnable et économique que le sujet d'une analyse d'impact de la protection des données soit plus large qu'un projet unique, par exemple lorsque les autorités publiques ou les organismes ont l'intention d'établir une plate-forme commune de traitement ou d'application ou lorsque plusieurs responsables de traitement envisagent d'introduire un environnement commun d'application ou de traitement dans un secteur ou segment industriel ou pour une activité horizontale largement utilisée ».

Cela signifie qu'une seul AIPD pourrait être utilisée pour évaluer des opérations de traitement multiples qui sont similaires en termes de risques présentés, compte tenu de la spécificité, de la portée, du contexte et des objectifs du traitement.

Le RGPD ne définit pas une AIPD ni la méthodologie à suivre mais précise son contenu minimum. Toute AIPD devra *au moins* contenir :

1. une description systématique des opérations de traitement envisagées (ce pourrait être réalisé en se basant sur le travail effectué pour le Registre des traitements) et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement, les destinataires envisagés des données et les catégories de données traitées.

   Cette description doit être complète, précise, cohérente et claire. Cette description ne pourra reprendre des finalités trop générales comme « Amélioration de l'expérience utilisateur » ou « Sécurité IT ». Il s'agit de donner une description claire et précise des traitements envisagés par le responsable ;

2. une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités.

   Il s'agit ici pour le responsable d'examiner l'efficacité du traitement envisagé (« Peut-on raisonnablement espérer que le traitement envisagé atteigne sa finalité ? ») et de veiller à maintenir un équilibre adéquat entre les intérêts pertinents ;

3. une évaluation des risques pour les droits et libertés des personnes concernées et

4. les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Lorsque l'opération de traitement implique des responsables de traitement conjoints, ils doivent définir leurs obligations respectives avec précision. L'AIPD devra indiquer lequel est responsable des différentes mesures conçues pour traiter les risques et protéger les droits des personnes concernées.

4. Qu'entend-on par « risque » ?

La notion de « risque » peut être envisagée de plusieurs façons.

Elle est généralement décrite comme la *possibilité* (« probabilité ») *qu'une menace déterminée se présente avec comme conséquence un impact déterminé* (« gravité »). Un « risque » est un scénario décrivant un événement et ses conséquences, le tout estimé en termes de « sévérité » et de « probabilité ». La gestion des risques (le « *Risk management* ») peut être défini comme l'activité d'une société qui a pour objet de la diriger d'une manière coordonnée en fonction de ses risques.

De quels risques l'article 35.1 du RGPD parle-t-il ?

Il renvoie à une catégorie particulière de risques à savoir les risques, non pas vis-à-vis de l'entreprise, mais vis-à-vis des droits et libertés des personnes physiques. Selon le Groupe de Travail « Article 29 », les termes « pour les droits et libertés des personnes physiques » du RGPD concernent principalement le droit au respect de la vie privée mais ils peuvent également se rapporter à d'autres droits et libertés fondamentaux comme la liberté d'expression, la liberté de pensée, de conscience et de religion, l'interdiction de discrimination et le droit à la liberté de mouvement.

Le considérant 75 du RGPD énumère, à titre d'exemple, un certain nombre de circonstances dans lesquelles les traitements engendrent des risques pour les droits et libertés des personnes physiques, et entraîner dans leur chef des dommages physiques, matériels ou un préjudice moral.

Il s'agit des possibilités suivantes :

1. lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important ;
2. lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel ;
3. lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou

des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes ;

4. lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels ;
5. lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants ; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.

Il est très important de toujours analyser/apprécier le risque en fonction des circonstances particulières de chaque traitement ou de chaque groupe de traitements.

L'analyse se doit d'être contextuelle. Il faut déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé pour les droits et libertés des personnes physiques.

5. Que veut dire « susceptible d'engendrer un risque élevé » pour les droits et libertés des personnes physiques ?

L'article 35.1 du RGPD précise quand il faut effectuer une AIPD :

> « Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires. ».

Toutefois, la notion « susceptible d'engendrer un risque élevé » n'est pas plus définie dans le RGPD.

Cette notion renvoie aux traitements de données dont il est vraisemblable qu'ils puissent avoir des *conséquences néfastes considérables* pour les libertés et droits fondamentaux des personnes physiques si on ne prend pas des mesures de protections adéquates. C'est particulièrement pertinent lorsqu'une nouvelle technologie de traitement de données est en train d'être mise en œuvre.

Une « conséquence considérable » signifie ici que, dans le cas où le risque se produirait, la personne concernée serait sensiblement touchée dans l'exercice ou la jouissance de ses droits et libertés fondamentaux. C'est, par exemple, le cas où il est vraisemblable que le traitement puisse engendrer les conséquences très négatives énumérées au considérant 75 du RGPD.

L'élément « susceptible d'engendrer un risque élevé » qui donne lieu à l'obligation de procéder à une AIPD concerne le risque inhérent au traitement de données envisagé. Et ce contrairement à l'article 36 du RGPD relatif à la consultation obligatoire de l'autorité de contrôle de protection des données personnelles qui lui concerne le risque résiduel.

Le risque « inhérent » renvoie à la probabilité qu'un impact négatif se produise si aucune mesure de protection n'est prise. Le risque « résiduel » concerne au contraire la probabilité qu'un impact négatif se produise malgré les mesures qui sont prises pour influencer ou limiter le risque (inhérent).

Dans les cas où la nécessité d'une AIPD n'est pas claire, le Groupe de Travail « Article 29 » recommande qu'une AIPD soit néanmoins effectuée. En effet, une AIPD est un outil utile pour aider les responsables de traitement à se conformer à la loi sur la protection des données.

Dans son texte, le RGPD cite en exemple les cas suivants en rapport avec la réalisation d'une AIPD (il s'agit de cas où le RGPD considère que les futurs traitements sont *susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques* et donc qu'une AIPD est obligatoire) :

1. l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
2. le traitement à grande échelle de catégories particulières de données visées à l'article 9.1 (données relatives à la santé par exemple), ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 du RGPD ou ;
3. la surveillance systématique à grande échelle d'une zone accessible au public.

Il s'agit là d'une liste non exhaustive qui sera amené à être précisée.

Les Lignes directrices du Groupe de Travail « Article 29 » précise les critères qui doivent être pris en considération lorsqu'un responsable de traitement doit se décider sur la réalisation ou non d'une AIPD.

Le responsable de traitement devrait tenir compte de plusieurs points :

1. le traitement envisagé concerne-t-il une évaluation ou une notation des personnes concernées, y compris leur profilage et de la prédiction, en particulier des « aspects concernant la performance du sujet de la personne sur le lieu de travail, la situation économique, la santé,

les préférences ou intérêts personnels, la fiabilité ou le comportement, l'emplacement ou les mouvements » (considérants 71 et 91 du RGPD) ? ;

2. s'agit-il d'une prise de décision automatisée avec effet juridique ou similaire ? Autrement dit, le traitement vise-t-il à prendre des décisions sur les personnes concernées produisant des « effets juridiques concernant la personne physique » ou « l'affectant de manière significative de façon similaire » (article 35.3.a du RGPD) ? Par exemple, le traitement peut entraîner l'exclusion ou la discrimination à l'égard des particuliers. Un traitement avec peu ou pas d'effet sur les individus ne correspond pas à ce critère spécifique ;
3. le traitement correspond-il en réalité à une surveillance systématique des personnes concernées c'est-à-dire un traitement réalisé pour observer, surveiller ou contrôler les personnes concernées, y compris d'une collecte de données recueillies par « un suivi systématique d'une zone accessible au public » ?

   Ce type de surveillance est un critère à ne pas oublier car les données personnelles peuvent être collectées dans des cas où les personnes concernées ne savent pas qui recueille leurs données et comment elles seront utilisées. En outre, il est souvent impossible pour les individus d'éviter d'être soumis à un tel traitement dans des espaces publics (ou accessibles au public) ;
4. le traitement envisagé traitera-t-il de données sensibles au sens de l'article 9 (par exemple les informations sur les opinions politiques des individus) ou 10 (données personnelles relatives aux condamnations ou aux infractions pénales) du RGPD ?

   Un exemple serait un hôpital qui conserverait les dossiers médicaux des patients ou un enquêteur privé qui conserverait des informations sur des délinquants. Ce critère comprend également des données qui peuvent généralement être considérées comme augmentant le risque éventuel pour les droits et les libertés des individus, tels que les données de communication électronique, les données de localisation, les données financières (qui pourraient être utilisées pour la fraude de paiement). À cet égard, le fait que les données aient déjà été publiées par la personne concernée ou par des tiers peut être pertinent ;
5. le responsable envisage-t-il de traiter des données à grande échelle ?

   Le RGPD ne définit pas ce qui constitue un traitement de données à grande échelle, mais son considérant 91 fournit toutefois des conseils.

   Le Groupe de Travail « Article 29 » recommande que les facteurs suivants, en particulier, soient pris en compte pour déterminer si le traitement est effectué à grande échelle :

   a) le nombre de personnes concernées, soit en tant que nombre spécifique, soit en proportion de la population concernée ;

b) le volume de données et/ou l'étendue de éléments de données traités ;

c) la durée, ou la permanence de l'activité de traitement de données ;

d) l'étendue géographique de l'activité de traitement ;

6. le traitement en question combinera-t-il ou pas des ensembles de données qui ont été rapprochés ou combinés à cet effet ? S'agira-t-il, par exemple, de données provenant de deux ou plusieurs traitements de données réalisés à des fins différentes et/ou par des responsables de traitement différents d'une manière qui dépasserait les attentes raisonnables de la personne concernée ? ;

7. le traitement visera-t-il des données concernant des personnes concernées dites vulnérables ?

   Le traitement de ce type de données peut nécessiter une AIPD en raison du déséquilibre de pouvoir accru entre la personne concernée et le responsable de traitement. En effet, ce type d'individu peut ne pas pouvoir consentir ou s'opposer au traitement de ses données. Par exemple, les employés rencontrent souvent de sérieuses difficultés pour s'opposer au traitement effectué par leur employeur, lorsqu'il est lié à la gestion des ressources humaines. De même, les enfants peuvent être considérés comme incapables de s'opposer sciemment et judicieusement au traitement de leurs données. Pour le Groupe de Travail « Article 29 », ce point concerne également un segment plus vulnérable de la population nécessitant une protection spéciale, par exemple, les malades mentaux, les demandeurs d'asile ou les personnes âgées, un patient ou tous les cas, où un déséquilibre dans la relation entre la personne concernée et le responsable de traitement peut être identifié ;

8. le traitement sera-t-il une utilisation innovante ou une mise en œuvre de solutions technologiques ou organisationnelles comme l'utilisation combinée de l'empreinte digitale et la reconnaissance faciale pour un meilleur contrôle d'accès physique, etc. ?

   Le RGPD indique clairement (article 35.1 et considérants 89 et 91) que l'utilisation d'une nouvelle technologie peut déclencher la nécessité d'effectuer une AIPD. En effet, l'utilisation de cette technologie peut impliquer de nouvelles formes de collecte et d'utilisation de données, éventuellement avec un risque élevé pour les droits et libertés des individus. Les conséquences personnelles et sociales du déploiement d'une nouvelle technologie peuvent être inconnues. Une AIPD aidera le responsable de traitement à comprendre et à traiter de tels risques. Par exemple, certaines applications de l'« Internet des objets » pourraient avoir un impact important sur la vie quotidienne et la vie privée des individus, et nécessitent donc une AIPD ;

9. le traitement en tant que tel empêchera-t-il les personnes concernées de pouvoir exercer l'un de leurs droits ou de bénéficier d'un service

ou d'un contrat ? Le traitement devrait-il permettre, modifier ou refuser l'accès des personnes concernées à un service ou de conclure un contrat ?

Le Groupe de Travail « Article 29 » cite en exemple le traitement effectué par une banque afin de confronter ses clients vis-à-vis d'une banque de données de référence relative aux crédits afin de décider si elle va leur octroyer un prêt ou non.

Selon le Groupe de Travail, dès qu'un traitement envisagé rencontre au moins deux des neuf critères énoncés plus haut, il est plus que probable qu'une AIPD soit nécessaire même s'il pourrait exister des situations où le traitement ne rencontre qu'un seul des critères et néanmoins nécessiter une AIPD.

Dans le cas où, selon l'analyse du Groupe de Travail, le traitement envisagé nécessite une AIPD et où le responsable du traitement décide de ne pas en réaliser une, il devra documenter cette décision ainsi que l'opinion de son DPD (s'il en dispose d'un bien sûr).

L'aide fournie par le Groupe de Travail est donc bienvenue même si, on le voit, tout est laissé à l'appréciation des responsables de traitement. On peut toutefois s'attendre à avoir bientôt plus d'informations sur le sujet de la part des différentes autorités de contrôle nationales. Espérons que ces informations ne soient pas contradictoires.

6. Les mesures envisagées pour faire face aux risques

Nous avons vu qu'une AIPD devra non seulement comprendre une appréciation des risques mais aussi une description des mesures envisagées pour faire face à de tels risques. Ces mesures peuvent être des mesures de sécurité, des garanties et des mécanismes pour assurer la protection des données à caractère personnel démontrant ainsi que le RGPD a été respecté.

Ce n'est qu'après la prise en considération de ces mesures que l'on peut valablement évaluer les risques résiduels des traitements envisagés.

7. Circonstances dans lesquelles une consultation préalable de l'autorité de contrôle des données personnelles est obligatoire

L'article 36.1 dispose à cet égard que :

« Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ».

Lorsque le responsable du traitement consulte l'autorité de contrôle, il devra lui communiquer :

1. le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises ;
2. les finalités et les moyens du traitement envisagé ;
3. les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu du présent règlement ;
4. le cas échéant, les coordonnées du DPD ;
5. l'analyse d'impact relative à la protection des données prévue à l'article 35 et ;
6. toute autre information que l'autorité de contrôle demande.

Les sociétés ne devront consulter les autorités de protection des données personnelles que si le risque « résiduel » est élevé.

Ce n'est que lorsqu'il s'avère que le traitement envisagé présenterait un risque élevé si le responsable ne prenait pas de mesures efficaces d'atténuation des risques que le traitement doit préalablement être soumis à l'autorité de contrôle.

Si la société peut limiter efficacement le risque à l'aide de mesures techniques et organisationnelles appropriées, aucune consultation préalable ne doit avoir lieu. Un exemple pourrait être le stockage des données personnelles sur les ordinateurs portables avec des mesures de sécurité techniques et organisationnelles appropriées (cryptage effectif du disque complet, gestion de clés robustes, contrôle d'accès approprié, sauvegardes sécurisées, etc.) en plus des politiques existantes (avis, consentement, droit d'accès, droit d'opposition, etc.). Les risques ayant été gérés par le responsable du traitement, le traitement peut être effectué sans consultation de l'autorité de contrôle compétente.

Lorsque les risques identifiés ne peuvent pas être suffisamment abordés par le responsable de traitement (autrement dit, les risques résiduels restent élevés), il doit consulter l'autorité de contrôle.

Un exemple d'un risque résiduel élevé inacceptable est le cas où les personnes concernées peuvent subir des conséquences importantes, voire irréversibles, des conséquences qu'elles ne pourraient pas surmonter et/ou lorsqu'il semble évident que le risque envisagé se produira.

En outre, le responsable de traitement devra consulter l'autorité de contrôle chaque fois que la législation de l'État membre exige que les responsables de traitement consultent et/ou obtiennent l'autorisation préalable de l'autorité de contrôle en relation avec le traitement par un responsable de traitement pour l'exécution d'une tâche effectuée par le responsable de traitement dans l'intérêt public, y compris le traitement relatif à la protection sociale et à la santé publique.

Si l'autorité de contrôle des données personnelles est d'avis que le traitement envisagé n'est pas conforme au RGPD, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle fournira par écrit, dans un délai de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant. Le RGPD ne précise pas la valeur de l'avis de l'autorité de contrôle nationale ni son contenu.

L'autorité pourra faire usage des pouvoirs visés à l'article 58 du RGPD.

Le délai de huit semaines pourra être prolongé de six semaines, en fonction de la complexité du traitement envisagé. L'autorité de contrôle devra informer le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard, dans un délai d'un mois à compter de la réception de la demande de consultation. Ces délais pourront être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation.

8. Méthodologie à appliquer pour réaliser une AIPD

Le responsable du traitement est libre d'utiliser la méthodologie qui lui convienne pour réaliser une AIPD du moment qu'elle respecte les exigences minimales du RGPD en matière d'objectivité et de confidentialité. En effet, le RGPD n'oblige à aucune méthodologie particulière en soi.

La méthodologie devra être adaptée aux besoins et au contexte de l'entreprise en question.

L'entreprise est encouragée à utiliser des normes internationales et des codes de conduite déjà approuvée. En effet, le respect d'un code de conduite doit être pris en compte lors de l'évaluation de l'impact d'une opération de traitement. Cela peut être utile pour démontrer que des mesures adéquates ont été choisies ou mises en place, à condition que le code de conduite soit approprié à l'opération de traitement.

Les exigences pertinentes énoncées dans le RGPD fournissent un cadre large et générique pour la conception et la réalisation d'une AIPD. Ces exigences peuvent être complétées par des conseils pratiques plus détaillés. Cela ouvre la voie à une certaine évolutivité et signifie aussi que même un petit responsable de traitement peut concevoir et implémenter une AIPD appropriée.

Le considérant 90 du RGPD décrit un certain nombre de composants de l'AIPD qui comprennent les composants bien connus de l'habituelle gestion des risques par une entreprise.

En termes de gestion des risques, une AIPD vise à « gérer les risques » vis-à-vis des droits et libertés des personnes physiques, en utilisant les trois processus suivants :

1. établir le contexte du traitement : « en tenant compte de la nature, de la portée et des finalités du traitement » ;

2. évaluer les risques : « évaluer la probabilité et la gravité particulières du risque élevé » ;
3. traiter les risques : « atténuer le risque » et « assurer la protection des données personnelles » et « démontrer le respect du présent règlement ».

Différentes méthodologies peuvent être utilisées pour aider à la mise en œuvre pratique des exigences de base énoncées dans le RGPD.

Afin de permettre l'existence de ces différentes approches, tout en permettant aux responsables de traitement de se conformer au RGPD, le Groupe de Travail « Article 29 » a identifié les critères communs de toute méthodologie en la matière. Le Groupe de Travail a considéré que ces critères étaient suffisants pour clarifier les exigences fondamentales du RGPD tout en offrant assez de possibilités pour différentes formes de mise en œuvre. La checklist du Groupe de Travail se retrouve en Annexe 2 de ses Lignes directrices du 4 octobre 2017.

Le Groupe de Travail « Article 29 » encourage le développement de procédures « AIPD » sectorielles. En effet, ces AIPD s'appuieront alors sur des connaissances sectorielles spécifiques. Nous sommes convaincus que l'élaboration de normes, d'AIPD, de certifications sectorielles est un marché d'avenir et que le secteur qui établira en premier des normes modèles et innovantes se développera plus rapidement que ceux qui auront encore à se positionner sur le sujet. Les normes les plus modernes et les plus rapidement mises sur le marché seront difficiles à éviter par la suite.

Formaliser l'analyse d'impact

Il convient de rapidement formaliser un processus visant à :

- analyser, pour chaque traitement, avant sa mise en œuvre ou avant toute modification, si une étude d'impact est nécessaire ;
- déterminer les modalités de l'analyse d'impact ;
- élaborer une procédure ou une méthode pour la réalisation de cette analyse d'impact, ainsi qu'une trame d'analyse associée ;
- déterminer les conséquences induites par cette analyse, en fonction du résultat obtenu, et
- prendre les mesures adaptées.

9. Contrôle

Le responsable du traitement est tenu de (faire) vérifier si le traitement est effectué conformément aux résultats de l'AIPD. Un tel contrôle, réalisé par le DPD, devra, au minimum, avoir lieu lorsque les moyens pour réaliser le traitement ont été modifiés, si l'état de la technique a évolué, en cas de découverte d'une défaillance ou d'une vulnérabilité dans la sécurité, si le/les risque(s) changent, etc.

Les risques évoluent vite toutefois.

C'est pourquoi, le Groupe de Travail considère comme de bonne pratique que les AIPD soient continuellement revues et régulièrement réévaluées.

Il serait bon qu'une liste en soit gardée auprès du DPD à charge pour lui de réaliser un contrôle régulier des traitements qui en ont découlé.

De plus, même si une AIPD n'était pas requise avant le 25 mai 2018, il sera nécessaire pour le responsable du traitement, à un certain moment, de réaliser une AIPD dans le cadre de ses obligations générales de conformité (« *accountability* »).

En effet, une AIPD est nécessaire pour les opérations de traitement déjà existantes qui changent de manière significative et dont le risque a évolué vers le haut. Les raisons d'une modification du risque sont multiples : changement de technologie vers une technologie plus intrusive, les personnes concernées par les décisions automatiques sont devenues plus vulnérables, etc.

C. Recommandation d'initiative de la Commission belge pour la protection de la vie privée concernant l'analyse d'impact relative à la protection des données (n° 01/2018 du 28 février 2018)

Le but de la recommandation est de fournir des explications plus détaillées concernant :

- les circonstances dans lesquelles une AIPD est obligatoire (section 3) ;
- les éléments essentiels d'une AIPD (section 5) ;
- les circonstances dans lesquelles une consultation préalable est obligatoire (section 6) ;
- les acteurs qui doivent être impliqués dans une AIPD (section 7) ;
- plusieurs dispositions particulières (section 8).

D. Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail a adopté (les lignes directrices du Groupe de Travail sont appelées à évoluer. Il faudra rester vigilant !) le 4 octobre 2017 des lignes directrices sur le sujet des AIPD.

Elles sont disponibles dans toutes les langues de l'Union européenne via le site du Groupe de Travail (« Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement (UE) 2016/679 », Réf. WP 248 rév. 01).

Fiche de guidance n° 11
Le Délégué à la Protection des Données (DPD)

Articles 37 à 39 du RGPD

Considérant 97 du RGPD

A. Principe

Le RGPD donne une place primordiale à un nouvel acteur en matière de protection des données à caractère personnel : le Délégué à la Protection des Données (ou DPD), plus couramment désigné en anglais sous le terme de *Data Protection Officer* (ou DPO).

Sa désignation n'est pas toujours obligatoire mais toujours (plus que) fortement conseillée.

En effet, lorsque les activités du responsable de traitement ou du sous-traitant consistent à traiter des données sensibles telles des données relatives à la santé, des données judiciaires mais aussi des données relatives à des mineurs à grande échelle, un DPD devra être désigné.

Cette désignation obligatoire s'impose aussi pour les autorités publiques et les organismes publics quelle que soit la nature des données traitées.

La fonction de DPD fait partie du principe d'*accountability*.

Chaque société doit, dès à présent, considérer les aspects pratiques de la désignation d'un DPD (ou de la fonction équivalente si un DPD n'est pas obligatoire) : où le DPD sera-t-il situé ? Comment aura-t-il accès à la gestion au plus haut niveau de la société ? Comment assurer son indépendance ? Comment les différents départements pourront-ils communiquer avec lui ? Comment peut-il se tenir informé des différents projets qui se développent dans sa société ?

Comment, pratiquement, pourra-t-il donner son « *privacy sign off* » aux projets ? Doit-il le donner une fois au début du développement des projets ou plusieurs fois ? Comment évaluer ses activités, le travail qu'il réalise pour la société ? Qui va l'évaluer à la fin de l'année ? Quels sont ses liens avec la fonction de *Compliance Officer* ? Avec la fonction de *Chief Information and Security Officer* ?

Les sociétés ne doivent pas hésiter à engager un DPD rapidement dans le cadre de leur mise en conformité avec le RGPD. En effet, cette mise en conformité pourra se faire avec son aide et soutien. Cela permet aussi d'éviter de le voir remettre en cause et en question des décisions que les sociétés ont prises auparavant sans sa présence.

B. Une désignation obligatoire dans trois cas de figure

Les institutions européennes ont placé le DPD au centre de la démarche de conformité des organismes et des sociétés. La démarche de conformité est vue comme un chemin qui ne s'arrête pas au 25 mai 2018. En effet, la mise en conformité pour mai 2018 n'est qu'une étape. C'est tout le temps que, par après, les sociétés devront veiller à respecter le RGPD et non pas juste une seule fois.

La désignation d'un DPD n'est pas toujours obligatoire.

Cette désignation, par le responsable du traitement et le sous-traitant, n'est en effet obligatoire que lorsque :

1. le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
2. les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ou ;
3. les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 (par exemple des données médicales) et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 du RGPD.

C'est clairement le point 2 qui est le plus difficile à comprendre. En effet, qu'est-ce qu'une activité de base ? Qu'est-ce qu'un suivi régulier et systématique à grande échelle ? Qu'est-ce qu'un traitement à grande échelle ?

Selon ce point 2, la désignation d'un DPD sera nécessaire lorsque la société réalise des opérations de traitement qui :

1. en tant qu'activités de base

Les activités doivent donc être inextricablement liées aux activités principales de la société (pas uniquement par exemple la simple gestion du *payroll* de ses employés) ;

2. du fait de leur nature,
3. de leur portée et/ou
4. de leurs finalités

Ainsi, le Groupe de l'Article 29 considère, par exemple, qu'une société de surveillance chargée d'assurer la sécurité d'un centre commercial ou de tout lieu ouvert au public devra désigner un délégué à la protection des données dans la mesure où son activité de surveillance implique *de facto* un traitement de données à caractère personnel ;

5. exigent un suivi régulier
6. et systématique (= utilisant un système)

   À ce sujet, le Groupe de l'Article 29 fait une interprétation large de la notion de suivi régulier et systématique des personnes de sorte que l'interprétation semble dorénavant désigner toutes les formes de suivi et de profilage dont la publicité comportementale. À titre d'illustration, le suivi de la position géographique des personnes dans le cadre de l'utilisation d'applications mobiles, les programmes de fidélité ou encore la surveillance et l'enregistrement de données dites de bien-être et d'état de forme à partir d'objets connectés seraient considérés comme un suivi régulier et systématique des personnes)
7. à grande échelle de personnes concernées.

   Ceci est à analyser au cas par cas et dépendra du nombre de personnes concernées, du volume des données, de la durée et de l'étendue du traitement, etc.

   Le considérant 91 du RGPD relatif à l'analyse d'impact apporte à ce sujet des éclaircissements. D'une part, il définit la notion *a contrario* en indiquant que : « Le traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel. ». Ainsi, le traitement de données à caractère personnel réalisé par un avocat ou un médecin exerçant son activité à titre individuel ne serait pas constitutif d'un traitement à grande échelle imposant la désignation d'un DPD. D'autre part, selon ce considérant, les opérations de traitement à grande échelle seraient celles qui « visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé (…) ».

   Dans ce contexte, le Groupe de l'Article 29 préconise de prendre en compte plusieurs critères parmi lesquelles le nombre de personnes concernées, le volume de données traitées, la durée des opérations de traitement ou encore l'étendue géographique des opérations de traitement. À titre d'illustration, le traitement de données à caractère personnel relatif aux déplacements des usagers d'un service de transport serait considéré comme un traitement à grande échelle.

Il convient de noter que le droit de l'Union et le droit national des Etats membres pourront prévoir des cas supplémentaires pour lesquels la désignation d'un DPD sera obligatoire.

C. Une désignation groupée

Un groupe d'entreprises pourra désigner un seul et unique DPD à condition que le DPD en question « soit facilement joignable à partir de chaque lieu d'établissement ». Le DPD devra être capable de communiquer dans la langue de l'autorité de contrôle de protection des données personnelles et des personnes concernées.

L'activité de DPD peut aussi ressortir d'un groupe de personnes, d'une équipe dédiée à ce sujet qui devra alors être régi par une description des activités de chacun.

Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

Dans les cas où la désignation n'est pas obligatoire, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peut désigner un DPD. Le DPD pourra alors agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

Notons que, dans ce cas, si la personne porte le titre de « DPD », elle sera soumise à l'ensemble des obligations du RGPD.

D. Qui peut être DPD ?

Le DPD est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions qui lui sont assignées par le RGPD (voir point suivant). À cet égard, une maitrise du Règlement européen mais également des textes sectoriels (voire régionaux ou communautaires en Belgique) impactant la protection des données personnelles est requise. Le Règlement prévoit en effet que certains domaines sont laissés à l'appréciation du droit national de chaque État membre.

Le DPD peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service (consultant).

Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.

Le DPD aura une tâche de pédagogie au sein de l'entreprise afin que chacun connaisse les enjeux de la nouvelle réglementation et l'applique au quotidien en particulier pour l'ensemble des traitements à venir. Il ne faut donc pas négliger les talents d'orateur et de conviction de la personne choisie.

E. Fonctions du DPD

Le DPD doit être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel de son organisation. Le DPD sera l'interlocuteur principal au sein de l'entreprise pour tout ce qui a trait à la protection des données personnelles.

L'application du RGPD impliquant d'importants changements organisationnels, le DPD pourra aider à coordonner la mise en œuvre des mesures nécessaires et faire le lien avec les salariés et les instances représentatives du personnel. Enfin le DPD pourra être amené à interagir en priorité avec les personnes dont les données sont traitées pour répondre à leurs questions et requêtes.

La consultation du DPD, qu'il soit interne ou externe à l'organisme, devra intervenir suffisamment en amont afin de lui permettre de formuler ses recommandations. Notons également que ces dernières devront être prises en compte. En cas de désaccord, le Groupe de travail « Article 29 » recommande que les raisons pour lesquelles les recommandations du DPD n'ont pas été suivies soient documentées. En outre, compte tenu de son positionnement, le DPD devra être consulté dans le cadre d'une violation de données ou de tout autre incident de sécurité, ce qui n'est pas sans lien avec le profil du DPD.

Il devra disposer des ressources nécessaires pour exercer ses missions et avoir accès aux données à caractère personnel et aux opérations de traitement de sa société. Il devra aussi pouvoir entretenir ses connaissances spécialisées (formations).

Il ne pourra recevoir aucune instruction en ce qui concerne l'exercice de ses missions de la part du responsable de traitement ou du sous-traitant.

Le DPD ne bénéficiera pas du statut de salarié protégé. Il ne pourra pas être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le DPD fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant. Il devra donc pouvoir accéder aux instances décisionnaires de son organisme (comité exécutif, secrétariat général, direction générale, etc.).

Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le RGPD.

La visibilité du DPD devra être renforcée par la publication de ses coordonnées à destination du public (site Internet institutionnel, site Internet marchand, intranet accessible aux salariés et/ou aux intervenants, documents émis par l'organisme, etc.).

Le Groupe de Travail « Article 29 » souligne que le Règlement européen n'exige pas que le nom du DPO soit communiqué aux personnes concernées. Toutefois, le Groupe considère que cela pourrait être une bonne pratique tout en laissant le soin au DPD et à l'organisme qui le désignera le soin de trancher cette question.

Le DPD est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres.

Le Règlement européen tient compte du fait que tous les organismes ne pourront pas consacrer un poste à plein temps de DPD. C'est pourquoi, le DPD pourra exécuter d'autres missions et tâches au sein de la société.

Toutefois, le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts. Il s'agit ici d'un point délicat car comment savoir quelle fonction un employé de la société exerçant la fonction de DPD par exemple à mi-temps dans son organisation peut exercer pour son autre mi-temps sans qu'il y ait de conflits d'intérêts ? Peut-il exercer aussi la fonction de CISO ? En tout état de cause, il s'agit d'éviter que le DPD soit aussi dans une position qui détermine les moyens et les finalités des traitements de l'entreprise (CEO, « Head of HR » ou « Head of IT »). Ce serait conflictuel.

Le Groupe de Travail « Article 29 » a identifié l'existence de conflits d'intérêts entre la fonction de DPD et des fonctions managériales (direction du département marketing, direction du département des ressources humaines, etc.). En tout état de cause, l'organisme devra veiller à ce que le DPD bénéficie du temps suffisant à l'exercice de ses missions.

F. Missions du DPD

De manière générale, le Groupe de Travail « Article 29 » encourage les entités/secteurs à définir des lignes directrices listant les situations dans lesquelles le DPD devra être désignées et consultées.

Ces documents pourront participer à la démonstration de la conformité de l'entité.

Le DPD a un rôle de sensibilisation et de communication renforcé. Les tâches et missions du DPD sont (au moins) les suivantes :

1. informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations

qui leur incombent en vertu du règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données.

Des textes importants en matière de protection des données à caractère personnel étant publiés à un rythme élevé aujourd'hui, le DPD devra réaliser une veille quotidienne sur le sujet.

Il pourrait aussi mettre en place des ateliers pédagogiques et d'échanges organisés pour les employés du responsable du traitement. Il pourrait (faire) écrire des articles à poster sur l'intranet de l'entreprise pour expliquer et détailler les grands principes du RGPD, illustrer le avant/après sur des cas concrets de traitements de données. L'information pourrait être diffusée sous la forme de vidéos, de podcasts… afin de faciliter l'appréhension et la compréhension de ces sujets hautement techniques. Pourquoi aussi ne pas poster des affichages et des flyers ciblés dans différentes salles dans le but de bien transmettre des messages ? Les possibilités sont multiples ;

2. contrôler le respect du RGPD, d'autres dispositions du droit de l'Union européenne ou du droit des États membres en matière de protection des données (son contrôle porte donc bien au-delà du RGPD) et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités de chaque intervenant impliqué dans la mise en œuvre des traitements, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;
3. dispenser des conseils, sur demande, en ce qui concerne l'AIPD et vérifier l'exécution de celui-ci. Le DPD devra vérifier que les analyses d'impact sont réalisées.

   Ses conseils pourront également être sollicités dans ce cadre. À la lecture des lignes directrices du Groupe de Travail « Article 29 », il ne s'agira pas d'*une simple vérification*.

   En effet, les autorités de contrôle recommandent que les conseils du DPD soient sollicités pour :

   - déterminer notamment si une analyse d'impact est ou non nécessaire ;
   - déterminer la méthodologie d'analyse à suivre ;
   - définir les mesures pour atténuer les risques pour les droits et libertés des personnes.

Si les recommandations du DPD ne sont pas prises en compte, le rapport d'analyse d'impact devra expressément contenir les motifs pour lesquels le responsable du traitement est passé outre ;

4. coopérer avec l'autorité de contrôle.

C'est la raison pour laquelle le Règlement européen prévoit que les coordonnées du DPD soient également communiquées à l'autorité de contrôle ;

5. faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36 du RGPD, et mener des consultations, le cas échéant, sur tout autre sujet.

On le voit, le DPD a plusieurs rôles : identifier les risques encourus par la société grâce aux informations qu'il reçoit et à l'actualité relative au secteur de sa société qu'il se doit de suivre, écrire, dans des termes facilement compréhensibles, les procédures de respect de la réglementation en ayant été impliqué à tous les niveaux décisionnels de la société et, enfin, contrôler que ce qu'il a préconisé a bien été respecté.

Le DPD a aussi de multiples missions : informer et conseiller les responsables de traitement, les sous-traitants et leurs employés sur les obligations qui leur incombent en vertu du RGPD et plus spécialement en cas de réalisation d'un AIPD, contrôler le respect de ces obligations (audit) et être la personne de contact de l'autorité de contrôle notamment en cas de violation de données personnelles.

G. Toujours cette notion de « risque »

Des compétences en matière de sécurité des données sont également exigées du DPD.

Le DPD devra tenir dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Les données, y compris personnelles, sont souvent collectées par une entreprise de manière massive et anarchique au détriment d'une approche stratégique et structurée.

L'entreprise se trouve alors souvent en possession de données de qualité médiocre, excessives et sous-exploitées.

Le DPD, en s'inscrivant dans une démarche de « gouvernance » des données, peut alors aider les organes de direction à définir une stratégie pérenne et pragmatique permettant d'exploiter au mieux ces données tout en restant garant de leur utilisation.

Le DPD constitue la preuve d'un comportement éthique de la société et contribue en cela à en valoriser l'image et à établir un cadre de confiance pour les partenaires. Il est fondamental pour une entreprise d'informer et d'impliquer au maximum son DPD dans ses processus opérationnels afin de d'éviter les sanctions, on le sait, importantes.

Bon à savoir : formaliser les missions du DPD

Le rôle du DPD doit être formalisé dans une lettre de mission ou *a minima* dans une fiche de poste détaillée dans la mesure où elle est fondamentalement transverse et peut, outre les missions expressément prévues par le règlement, recouvrir divers aspects complémentaires.

En pratique, le DPD devrait principalement être amené à intervenir :

- en amont de la mise en œuvre d'un nouveau traitement pour identifier l'ensemble des actions à déployer pour que ce traitement soit implémenté conformément aux dispositions légales et réglementaires applicables (respect des principes de licéité, de limitation des finalités, de transparence et d'information des personnes concernées, de minimisation des données, de limitation de la conservation, vérification de l'adéquation des mesures de sécurité, etc.) ;
- dans le cycle de vie des traitements, notamment en procédant à la définition de mécanismes de vérification de la conformité ou encore à des audits pour contrôler le respect des obligations issues du RGPD ;
- pour sensibiliser les acteurs pouvant être amenés à traiter des données à caractère personnel, notamment au moyen de l'élaboration d'une politique SIF (sensibilisation – information – formation) dédiée à la thématique « Protection des données à caractère personnel » (ex : newsletter du DPD, page intranet dédiée, sessions de formation et e-learning, procédures internes, etc.) ;
- pour échanger avec l'autorité de contrôle nationale, voire répondre aux demandes de cette dernière le cas échéant, notamment dans le cadre de consultations (obligatoires ou non) ;
- pour répondre aux questions, réclamations ou demandes d'exercice de leurs droits par les personnes concernées ;
- dans le cadre d'autres missions pouvant parfois être mises à sa charge telles que la tenue du registre des traitements, le maintien d'une documentation « Protection des données à caractère personnel » dédiée ou encore la réalisation de bilans ou de rapports réguliers s'agissant de son activité, etc.

H. Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail « Article 29 » a adopté le 5 avril 2017 des Lignes directrices en rapport avec le DPD.

Ces Lignes directrices sont disponibles via le site internet du Groupe de Travail dans toutes les langues de l'Union européennes (« Lignes directrices concernant les délégués à la protection des données (DPD) », Réf. WP 243 rev.01).

Fiche de guidance n° 12
Les codes de conduite

Articles 24, 28(5), 32, 40, 41, 57, 58, 64, 70 & 83 du RGPD

Considérants 74 à 77, 81, 83, 84, 98, 99, 100, 129 à 131, 139, 140, 148 à 151, 158, 167 & 168 du RGPD

A. Introduction

Instruments encore méconnus de la pratique juridique (mais pas informatique), les codes de conduite, certifications, labels et marques ou encore les règles contraignantes d'entreprise, pourraient se révéler être des outils précieux pour guider les organisations dans leurs efforts de conformité, en leur fournissant un cadre de conformité plus adapté et personnalisé que les règles génériques du RGPD.

Dans une acception large, un code de conduite pour une entreprise ou un groupe d'entreprises voire un secteur d'activité est un ensemble d'engagements unilatéraux sur des principes, des actions, des pratiques, sur une conduite que cette entreprise, groupe d'entreprises ou secteur s'engage à adopter et respecter, le tout formalisé au sein d'un document rendu public.

On le comprend, un code de conduite n'est pas imposé par une loi ou une réglementation. Sa valeur contraignante ne vient donc pas de la sanction prévue par la loi, mais du caractère public de l'engagement unilatéral pris par l'entreprise qui, en cas de non-respect de cet engagement, se retrouve publiquement exposée et décrédibilisée.

Popularisé par les stratégies et plans de responsabilité sociétale et environnementale des entreprises, cet outil parfois conçu et perçu comme un simple instrument de communication et de marketing est le plus souvent un véritable instrument normatif pour les entreprises dans un contexte de « *soft law* », à savoir d'autorégulation, de plus en plus prégnant et encouragé par le législateur national et européen lui-même.

Le RGPD ne contient pas, dans sa partie normative, de définition de ce qu'il faut entendre par « code de conduite ». L'article 40.1 l'évoque non pas à l'échelle d'une entreprise mais d'un secteur d'activité donné, secteur qui se doterait d'un ensemble de règles destinées à « contribuer à la bonne application du RGPD, compte tenu de la spécificité des différents secteurs de traitement ».

C'est donc un code de conduite « sectoriel » que vise le RGPD.

Le considérant 77 énonce lui que les codes de conduite peuvent contenir :

« des directives relatives à la mise en œuvre de mesures appropriées et à la démonstration par le responsable du traitement ou le sous-traitant du respect du présent règlement, notamment en ce qui concerne l'identification du risque lié au traitement, leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et l'identification des meilleures pratiques visant à atténuer le risque. ».

Lors de leur élaboration, les codes de conduite devront tenir compte des spécificités des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises.

B. Utilités

L'application d'un code de conduite peut servir d'élément pour démontrer :

1. le respect des obligations incombant au responsable du traitement (son *accountability* par exemple) ;
2. l'existence des garanties suffisantes exigées dorénavant aux sous-traitants ;
3. le respect des exigences relatives à la sécurité des traitements.

L'adhésion à un code de conduite est aussi prise en compte dans les analyses d'impact en ce qu'elle permet de minimiser les risques liés aux traitements réalisés.

Par ailleurs, l'adhésion à un code de conduite par un responsable du traitement ou un sous-traitant est incluse parmi les « circonstances atténuantes » devant être prises en compte par les autorités de contrôle en cas de décision de sanction administrative. Ainsi, le montant d'une telle sanction administrative pourra être diminué si l'entreprise concernée démontre qu'elle respecte un code de conduite approuvé.

Enfin, l'adhésion à un code de conduite (comme c'est aussi le cas en ce qui concerne les certifications) permet à des prestataires étrangers de fournir des « garanties appropriées » dans le cadre d'un transfert de données, sous réserve d'un engagement juridiquement contraignant sur ces garanties. C'est une option intéressante qui peut être proposée à des partenaires hors UE (tels que des prestataires américains).

Si un secteur déterminé s'organise pour développer et faire valider un code de conduite, dont l'adhésion sera ensuite proposée aux entreprises concernées dans les conditions permettant le plein effet juridique du code de conduite sectoriel, ces entreprises pourraient bénéficier des économies d'échelle générées par une telle démarche collective.

Pour le législateur, c'est le moyen de permettre au plus grand nombre d'entreprises d'accéder aux outils de conformité, mais aussi de pouvoir dialoguer directement avec les instances représentatives des secteurs qui auront adopté un code de conduite, réduisant ainsi le nombre d'interlocuteurs directs.

C. Procédure

Les codes de conduite sectoriels, pour produire leur plein effet, doivent avoir suivi une procédure d'approbation précise visant à garantir leur conformité à la réglementation européenne.

Les codes de conduite seront élaborés par les associations et les autres organismes représentant des catégories de responsables du traitement ou de sous-traitants.

Ce sont ces mêmes entités qui pourront par après les modifier ou les proroger.

Les associations et autres organismes qui ont l'intention d'élaborer un code de conduite (voire de modifier ou proroger un code de conduite existant) doivent d'abord soumettre le projet de code, de modifications ou de prorogation à leur autorité de contrôle des données personnelles.

1. Le projet de code ne porte pas sur des activités de traitement menées dans plusieurs États membres

Dans ce cas, la procédure reste purement nationale.

Ce sera uniquement l'autorité de contrôle nationale qui devra rendre un avis sur la question de savoir si le projet de code, de modification ou de prorogation respecte le RGPD. Elle approuvera ce projet de code, cette modification ou cette prorogation si elle estime qu'il offre des garanties appropriées suffisantes.

Lorsque le projet de code, la modification ou la prorogation est approuvé par l'autorité, celle-ci enregistre et publie le code de conduite.

2. Le projet de code de conduite concerne des activités de traitement menées dans plusieurs États membres

Lorsque le projet de code de conduite concerne des activités de traitement menées dans plusieurs États membres, l'autorité de contrôle saisie devra soumettre le projet de code, la modification ou la prorogation, avant approbation, au Comité européen de la protection des données (le CEPD). Celui-ci devra rendre un avis sur la question de savoir si le projet de code, la modification ou la prorogation respecte bien le RGPD.

Lorsque le CEPD confirme que le projet de code, la modification ou la prorogation respecte le RGPD, le comité soumet son avis à la Commission européenne.

La Commission européenne peut décider, par voie d'actes d'exécution, que le code de conduite, la modification ou la prorogation approuvés qui lui ont été soumis sont d'application générale au sein de l'Union européenne.

La Commission européenne veillera à garantir une publicité appropriée aux codes approuvés dont elle a décidé qu'ils sont d'application générale.

D. Champ d'application des futurs codes de conduite

Les associations représentatives des responsables du traitement ou des sous-traitants pourront proposer des codes de conduite dans tous les domaines du RGPD comme, par exemple, concernant :

1. le traitement loyal et transparent ;
2. les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques ;
3. la collecte des données à caractère personnel ;
4. la pseudonymisation des données à caractère personnel ;
5. les informations communiquées au public et aux personnes concernées ;
6. l'exercice des droits des personnes concernées ;
7. les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant ;
8. les mesures et les procédures visées imposés par le *privacy by design* et par le *privacy by default* ainsi que les mesures visant à assurer la sécurité du traitement ;

9. la notification aux autorités de protection des données personnelles des violations de données à caractère personnel et la communication de ces violations aux personnes concernées ;
10. le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales ;
11. les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement.

Les différents États membres, les autorités de contrôle des données personnelles, le CEPD et la Commission européenne encourageront l'élaboration de ces codes de conduite.

E. Contrôle du respect du code de conduite

Les codes de conduite ne devront pas être de simples stipulations sans aucune valeur.

En effet, les codes de conduite devront obligatoirement comprendre des mécanismes et des procédures permettant à un organisme indépendant de procéder régulièrement au contrôle obligatoire de ses dispositions et engagements par les responsables du traitement ou les sous-traitants qui se sont engagés à les respecter et à les appliquer.

L'organisme agréé pourra prendre les mesures appropriées en cas de violation par un responsable du traitement ou un sous-traitant du code de conduite en question tout en veillant à ce que ce responsable soit en mesure de se défendre. L'organisme pourra notamment suspendre ou exclure le responsable du traitement ou le sous-traitant concerné de l'application du code. Il informera l'autorité de contrôle compétente de ces mesures et des raisons pour lesquelles elles ont été prises.

L'organisme de contrôle du code de conduite devra avoir été accrédité à cet effet par une autorité de contrôle des données personnelles.

L'organisme devra disposer d'un niveau d'expertise approprié au regard de l'objet du code de conduite.

Il sera agréé pour contrôler le respect d'un code de conduite lorsqu'il a :

1. démontré, à la satisfaction de l'autorité de contrôle, son indépendance et son expertise au regard de l'objet du code ;
2. établi des procédures qui lui permettent d'apprécier si les responsables du traitement et les sous-traitants concernés satisfont aux conditions pour appliquer le code, de contrôler le respect de ses dispositions et d'examiner périodiquement son fonctionnement ;

3. établi des procédures et des structures pour traiter les réclamations relatives aux violations du code ou à la manière dont le code a été ou est appliqué par un responsable du traitement ou un sous-traitant, et pour rendre ces procédures et structures transparentes à l'égard des personnes concernées et du public et
4. démontré, à la satisfaction de l'autorité de contrôle, que ses tâches et ses missions n'entraînent pas de conflit d'intérêts.

L'autorité de contrôle des données personnelles compétente devra soumettre le projet de critères d'agrément d'un organisme au CEPD en application du mécanisme de contrôle de la cohérence du RGPD.

L'autorité de contrôle des données personnelles révoquera l'agrément d'un organisme si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organisme constituent une violation du RGPD.

F. Rôles des autorités de protection

Chaque autorité de contrôle, sur son territoire, devra :

- encourager l'élaboration de codes de conduite ;
- rendre un avis et approuver les codes de conduite qui fournissent des garanties suffisantes ;
- rédiger et publier les critères d'agrément pour les organismes qui veulent contrôler le suivi des codes de conduite ;
- procéder à l'agrément des organismes chargés du suivi des codes de conduite.

Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative en cas de violation du RGPD, l'autorité de contrôle concernée tiendra dûment tenu compte de l'application ou non de codes de conduite.

G. Autres rôles du CEPD

On l'a vu, le CEPD intervient dans l'approbation, la modification ou la prorogation de codes de conduite qui concerneront plusieurs États membres. À cet effet, l'autorité de protection compétente devra à chaque fois communiquer le projet de décision au CEPD.

Il devra aussi consigner dans un registre tous les codes de conduite, les modifications et les prorogations approuvés et les mettre à la disposition du public par tout moyen approprié.

Le CEPD veille à l'application cohérente du RGPD. À cet effet, le CEPD, de sa propre initiative ou, le cas échéant, à la demande de la Commission européenne, émettra des avis sur les codes de conduite qui ont été déclarés d'application générale au sein de l'Union européenne par la Commission européenne.

H. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 13 : La labellisation et la certification*
- *Fiche de guidance n° 31 : Le CEPD (le « Comité européen de la protection des données »)*

Fiche de guidance n° 13
La labellisation et la certification

Articles 24, 25, 28, 32, 42 et 43 du RGPD

Considérants 74 à 78, 81, 83, 84, 100 du RGPD

A. Introduction

Dans le but de favoriser la transparence et le respect du RGPD, la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données sera de plus en plus encouragée par les différents États membres, les autorités de contrôle, le CEPD et la Commission européenne, ceci afin de permettre aux personnes concernées d'évaluer très rapidement le niveau de protection des données offert par les produits et services d'une société (considérant 100 du RGPD).

Mais que sont exactement ces « mécanismes de certification », ces « labels » et ces « marques » ?

Une certification est une évaluation appropriée d'un traitement par un organisme de certification. Son analyse conduit à la délivrance (ou non) par ledit organisme de son approbation sur la conformité du traitement analysé par rapport au RGPD.

B. Utilités des certifications, labels et marques

Ces instruments peuvent être utilisés (mais ce n'est pas une obligation) par des responsables du traitement et par des sous-traitants soumis au RGPD pour démontrer que leurs activités de traitement que ce soit pour certains ou pour l'ensemble de leurs services, produits ou activités, respectent le RGPD. Une certification ne diminuera jamais la responsabilité du responsable du traitement ou du sous-traitant quant au respect du RGPD. De plus, ce n'est pas parce

qu'une société possède une certification qu'elle ne sera pas ou plus contrôlée par les autorités de contrôle des données personnelles.

Ces mécanismes peuvent également être utilisés pour démontrer l'existence de garanties appropriées pour les responsables de traitement ou sous-traitants n'entrant pas dans le champ d'application du RGPD ou dans le cadre de transfert de données vers des États tiers en l'absence de décision d'adéquation.

De plus, l'adhésion à un mécanisme de certification peut être prise en compte par l'autorité de contrôle en cas de sanctions. Autrement dit, la certification aura vraisemblablement un effet atténuant sur de potentielles sanctions dans la mesure où le responsable du traitement ou le sous-traitant aura respecté les prescriptions de la certification. C'est aussi un gage de confiance pour les responsables de traitement devant choisir des sous-traitants présentant des garanties suffisantes de protection des données.

Un mécanisme de certification approuvé en vertu de l'article 42 du RGPD peut servir d'élément pour démontrer en particulier :

1. le respect des exigences du *privacy by default* et de la *privacy by design* ;
2. l'existence des garanties suffisantes exigées à un sous-traitant ;
3. le respect des exigences relatives à la sécurité des traitements.

C. Procédure

La certification devra toujours être accessible via un processus transparent.

La certification peut être délivrée par :

1. des organismes de certification sur la base de critères approuvés par une autorité de contrôle compétente ;
2. l'autorité de contrôle nationale compétente sur la base de critères qu'elle aura elle-même approuvés ;
3. le Comité européen de la protection des données (CEPD).

Lorsque les critères de délivrance de la certification ont été approuvés par le CEPD, la certification portera le titre de « label européen de protection des données ».

Les critères de certification seront rendus aisément accessibles par les autorités de protection des données personnelles (qui devront les transmettre au CEPD).

L'adhésion à un mécanisme de certification est volontaire et transparente. Le responsable du traitement ou le sous-traitant qui soumet son traitement au mécanisme de certification devra fournir à l'organisme de certification ou à l'autorité de contrôle compétente toutes les informations et l'accès à ses activités de traitement afin de permettre que la procédure de certification soit réalisée correctement.

D. Retrait de la certification

La certification peut être retirée, s'il y a lieu, par les organismes de certification ou par l'autorité de contrôle compétente lorsque les exigences applicables à la certification ne sont pas ou plus satisfaites.

Les organismes de certification informent les autorités de contrôle des données personnelles pour qu'elle puisse au besoin retirer une certification, ordonner à l'organisme de certification de retirer une certification déjà délivrée ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites.

Les organismes de certification communiquent aussi aux autorités de protection des données personnelles les raisons de la délivrance ou du retrait de la certification demandée.

E. Durée de la certification

La certification est délivrée à un responsable du traitement ou à un sous-traitant pour une durée maximale de trois ans. La certification pourra être renouvelée dans les mêmes conditions dans le cas où le responsable/sous-traitant continue à respecter les conditions de la certification.

F. Registre des mécanismes de certification

Le CEPD est chargé de consigner dans un registre particulier tous les mécanismes de certification et les labels ou les marques en matière de protection des données. Le CEPD devra mettre à la disposition du public ce registre, par exemple via son site internet.

G. L'organisme de certification

Nous l'avons vu, les certifications peuvent être délivrées par des organismes de certification.

Qui pourra se prétendre « organisme de certification » ?

L'organisme en question devra disposer d'un niveau d'expertise approprié en matière de protection des données.

L'entité devra demander à être agréée en tant que tel par :

a) une autorité de contrôle des données personnelles ;

b) l'organisme national d'accréditation désigné conformément au règlement (CE) n° 765/2008 du Parlement européen et du Conseil, conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle des données personnelles.

Les entités qui demandent à être agréées ne le seront que lorsqu'elles ont :

a) démontré, à la satisfaction de l'autorité de contrôle des données personnelles, leur indépendance et leur expertise au regard de l'objet de la certification ;

b) pris l'engagement de respecter les critères établis pour la certification demandée et approuvés par l'autorité de contrôle des données personnelles ou par le CEPD ;

c) mis en place des procédures en vue de la délivrance, de l'examen périodique et du retrait d'une certification, de labels et de marques en matière de protection des données ;

d) établi des procédures et des structures pour traiter les réclamations relatives aux violations de la certification ou à la manière dont la certification a été ou est appliquée par un responsable du traitement ou un sous-traitant, et pour rendre ces procédures et structures transparentes à l'égard des personnes concernées et du public et

e) démontré, à la satisfaction de l'autorité de contrôle des données personnelles, que leurs tâches et leurs missions n'entraînent pas de conflit d'intérêts dans leur chef.

L'agrément des organismes de certification se fait sur la base de critères approuvés par l'autorité de contrôle des données personnelles ou par le CEPD. Les exigences pour pouvoir être agréé seront rendues aisément accessibles par les autorités de protection des données personnelles (qui devront aussi les transmettre au CEPD).

L'agrément est délivré pour une durée maximale de cinq ans et peut être renouvelé dans les mêmes conditions tant que l'organisme de certification satisfait aux exigences voulues.

L'autorité de contrôle des données personnelles ou l'organisme national d'accréditation pourra révoquer l'agrément d'un organisme de certification si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organisme de certification constituent une violation du RGPD.

H. Contrôle des autorités de contrôle des données personnelles

Sans préjudice de leurs autres missions prévues dans le RGPD, chaque autorité de contrôle nationale des données personnelles, sur son territoire :

- encouragera la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données ;
- approuvera les critères de certification pour qu'un organisme de certification puisse délivrer (ou pas) une certification ;
- procèdera, le cas échéant, à l'examen périodique des certifications délivrées par les organismes de certification ;
- rédigera et publiera les critères pour qu'un organisme puisse obtenir son agrément en tant qu'organisme de certification ;
- procèdera à l'agrément des organismes qui désirent devenir organismes de certification ;
- pourra retirer une certification ou ordonner à l'organisme de certification de retirer une certification déjà délivrée ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites ;
- pourra aussi délivrer des certifications en tant qu'organisme de certification.

Dans le cas où une autorité de contrôle des données personnelles voudrait imposer une amende administrative, elle devra tenir compte de l'application de mécanismes de certification.

I. Rôle du CEPD

On le sait, le CEPD veille à une application cohérente du RGPD sur l'ensemble des États membres.

À ce titre, il émettra un avis chaque fois qu'une autorité de contrôle des données personnelles envisage (à cet effet, l'autorité de contrôle compétente communiquera le projet de décision au CEPD) d'approuver les critères d'agrément des futurs organismes de certification.

De plus, le CEPD, de sa propre initiative ou à la demande de la Commission européenne, devra :

- encourager la mise en place de mécanismes de certification et de labels et de marques en matière de protection des données ;
- procéder à l'agrément des organismes de certification et à l'examen périodique de leur agrément ;

- tenir à jour un registre public des organismes agréés ;
- définir les exigences pour qu'un organisme puisse être agréé par le CEPD ;
- rendre à la Commission européenne un avis sur les exigences en matière de certification dans le cas où la Commission désire adopter un acte qui concerne les mécanismes de certification en matière de protection des données.

J. Des lignes directrices officielles

Malgré la complexité et la diversité du dossier, des lignes directrices en matière d'accréditation de tiers certificateurs et de certification devraient tout même être adoptées prochainement. Il y eut un premier atelier de travail du Groupe de Travail « Article 29 » en avril 2017 sur le sujet.

Les lignes directrices devront définir qui certifie (et comment) qu'une solution ou un fournisseur IT est bien « RGPD compatible ». La dimension technique (voire politique) est ici aussi forte que la dimension juridique.

Le RGPD consacre l'existence d'organismes agréés par l'État (ou par son représentant, comme la CPVP en Belgique ou la CNIL en France). Autrement dit, les autorités de protection des données personnelles pourront donner une accréditation qui permettra de déléguer à des tiers – *a priori* privés – cette mission de certification des solutions informatiques. Toutefois, rien ne dit que ce ne seront pas les autorités elles-mêmes qui donneront ces labels comme la CNIL française le fait depuis 2012.

Les lignes directrices devront déterminer les critères exacts d'évaluation de ces intermédiaires ainsi que les critères d'audit des solutions (logiciels, cloud, matériels) qui seront analysées par eux.

K. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 12 : Les codes de conduite*
- *Fiche de guidance n° 31 : Le CEPD (le « Comité européen de la protection des données »)*

Fiche de guidance n° 14
Les transferts de données

Chapitre V du RGPD (Articles 44 à 50)

Considérants 6, 29, 101 à 116 & 123 du RGPD

A. Principe

Les transferts de données personnelles hors de l'Union européenne et plus spécifiquement outre-Atlantique sont au cœur de l'actualité. En effet, ces transferts sont essentiels au bon développement et à l'expansion des activités des géants du web et nécessaires au bon fonctionnement du commerce international ainsi qu'à la coopération internationale.

Les règles actuellement en vigueur en matière de transfert de données personnelles sont pour leur grande majorité reprises aux articles 44 et suivants du Règlement.

Une société ne peut réaliser un transfert de données à caractère personnel (autrement dit, un transfert hors UE ou vers une organisation internationale) que si certaines garanties sont réalisées garantissant les droits et libertés des personnes ainsi que la protection de leurs données à caractère personnel.

Ces garanties sont les suivantes :

1. une décision d'adéquation de la Commission européenne ;
2. la fourniture de garanties appropriées qui peuvent être :
   a) des clauses types de protection des données adoptées ou approuvées par la Commission ;
   b) un code de conduite ou une certification ;
   c) des clauses contractuelles adaptées entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel dans le pays tiers mais sous réserve d'une autorisation par leur autorité de contrôle nationale ;

d) des règles d'entreprise contraignantes (les fameuses *Binding Corporate Rules* ou « BCR ») ;

3. à défaut de décisions d'adéquation ou de garanties appropriées, les transferts demeurent possibles pour certaines situations particulières.

Ces dérogations sont strictement encadrées et reposent sur des conditions qui seront difficiles à remplir ou à démontrer (par exemple : le consentement explicite de la personne concernée qui a été préalablement informée des risques liés au transfert ou lorsque le responsable du traitement prétend que le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat bénéficiant à la personne concernée).

Les règles sur le sujet veillent à ce que le niveau de protection garanti aux Européens par le RGPD ne soit pas compromis ni diminué.

B. Définition

Un « transfert » est une transmission de données personnelles collectées auprès d'un citoyen européen vers un pays tiers ou vers une organisation internationale où elles sont censées y faire l'objet d'un traitement après ledit transfert. Le RGPD ne contient pas de définition de ce qu'il faut entendre par « pays tiers ». C'est assez surprenant. L'article 45.8 du RGPD contient juste le renvoi vers la liste des pays pour lesquels elle a constaté par voie de décision qu'un niveau de protection adéquat est ou n'est plus assuré.

En pratique : illustrations de transferts de données ou de flux transfrontières

Il peut par exemple s'agir :

- de la centralisation intra-groupe, dans un pays hors Union européenne, de la base de données de gestion des commandes et de la comptabilité client ;
- de la centralisation intra-groupe, dans un pays hors Union européenne, de la base de données de gestion des ressources humaines d'un groupe multinational ;
- du transfert de dossiers contenant des données personnelles vers un prestataire situé dans un pays hors Union européenne, aux fins de saisies informatiques ;
- du recours à un centre d'appel hors Union européenne et d'un transfert du fichier correspondant pour le démarchage de clients ou des opérations de qualification ;
- de l'hébergement et de l'exploitation de plates-formes informatiques dans un pays hors Union européenne ;
- de systèmes internationaux de maintenance informatique faisant appel à des ressources hors Union européenne.

Un tel transfert ne peut se réaliser sans respecter l'ensemble des dispositions du RGPD dont, en particulier, celles écrites concernant ce genre de transmissions.

Le considérant 102 du RGPD précise que l'Union européenne peut aussi conclure des accords internationaux avec des pays tiers en vue de régler la protection des données personnelles lorsque des données doivent être transférées

de l'Union vers ce pays tiers. Les pays de l'Union peuvent aussi conclure individuellement de tels accords. Toutefois, ces accords ne pourront aller contre les règles inscrites dans le RGPD qui doit rester le socle commun et de base.

C. Interdiction de réaliser des transferts

Cela peut paraître surprenant mais le RGPD commence par préciser que, par principe, ce genre de traitement (le transfert) ne peut avoir lieu.

Toutefois, continue le RGPD, le transfert peut se réaliser si certaines conditions (qu'il énonce directement par après) sont réalisées. Il faudra donc d'abord analyser si les conditions du transfert existent avant de le réaliser.

D. Transferts fondés sur une décision d'adéquation

Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut tout d'abord avoir lieu si la Commission européenne a constaté par voie de décision que le pays tiers, un territoire, un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat.

Dès lors que la Commission européenne a pris une telle décision d'adéquation, les transferts futurs vers les pays concernés/organisations ne nécessitent pas d'autorisation spécifique préalable. Toutefois, et il est bon de le rappeler, cela n'empêchera pas le traitement envisagé de devoir respecter toutes les autres dispositions du RGPD (base juridique, principes généraux, etc.).

1. Mécanisme de la prise de décision

Lorsqu'elle désirera prendre une décision d'adéquation, la Commission européenne devra analyser la situation de la protection des données à caractère personnel dans le pays en question.

Lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission européenne devra tenir compte, en particulier, des éléments suivants :

1. l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux

données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées ;

2. l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer, y compris par des pouvoirs appropriés d'application desdites règles, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle des États membres et
3. les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

La Commission européenne, après avoir évalué le caractère adéquat du niveau de protection, décidera qu'un pays tiers particulier, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, assure bien un niveau de protection adéquat.

2. Modifications possibles des décisions

La décision de la Commission européenne prévoira un mécanisme d'examen périodique, au moins tous les quatre ans, qui devra prendre en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale.

La Commission européenne s'est engagée à suivre, de manière permanente, les évolutions dans les pays tiers et au sein des organisations internationales qui bénéficient d'une décision d'adéquation afin de voir si ces pays ou organisations n'ont pas pris de mesures qui pourraient porter atteinte au fonctionnement des décisions adoptées tant sur la base du RGPD que de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données d'ailleurs.

Lors la surveillance des décisions d'adéquation et de la réalisation des examens périodiques, la Commission prendra en considération les observations et les conclusions du Parlement européen et du Conseil, ainsi que d'autres organes et sources pertinents.

Lorsque les informations disponibles révèlent qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat, la Commission européenne pourra si nécessaire, abroger, modifier ou suspendre la décision d'adéquation par voie d'actes d'exécution sans effet rétroactif.

Pour des raisons d'urgence impérieuses dûment justifiées, la Commission pourra d'ailleurs adopter des actes d'exécution immédiatement applicables.

Dans le cas où la Commission européenne entend abroger, modifier, suspendre une décision d'adéquation ou prendre un acte immédiatement applicable, elle devra engager rapidement des consultations avec le pays tiers ou l'organisation internationale en vue de remédier à la situation. La Commission européenne devra fournir au pays tiers ou à l'organisation concerné toutes les informations nécessaires sur sa décision.

La décision d'abrogation, de modification, de suspension ou l'acte d'exécution immédiat est sans préjudice des transferts de données à caractère personnel vers le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou à l'organisation internationale en question, effectués en application des autres possibilités de garanties prévues dans le RGPD (BCR, clauses-types, etc.).

Dans le cas d'une décision d'abrogation par la Commission européenne d'une décision d'adéquation, les transferts réalisés uniquement sur cette base juridique deviendraient directement illicites. Nous conseillons donc aux sociétés qui réalisent des transferts vers les pays bénéficiant de telles décisions (voyez la liste ci-dessous) de suivre la doctrine de la Commission européenne sur ce point afin de pouvoir réagir rapidement s'il le faut (changer de base juridique, modifier le pays bénéficiant des transferts, etc.).

3. Publication des décisions

La Commission publiera au *Journal officiel de l'Union européenne* et sur son site internet une liste des pays tiers, des territoires et des secteurs déterminés dans un pays tiers et des organisations internationales pour lesquels elle a constaté par voie de décision qu'un niveau de protection adéquat est ou n'est plus assuré.

Les décisions adoptées par la Commission sur la base de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation par une décision de la Commission adoptée conformément cette fois-ci au RGPD.

À ce jour, les pays reconnus par une décision d'adéquation comme offrant un niveau suffisant de protection des données à caractère personnel sont les suivants :

- la Suisse ;
- le Canada ;
- l'Argentine ;
- Guernesey ;
- l'Ile de Man ;
- Jersey ;
- Andorre ;
- les Iles Féroé ;
- Israël ;
- l'Uruguay ;
- la Nouvelle-Zélande.

Les États de l'Espace économique européen (la Norvège, l'Islande et le Lichtenstein) sont également considérés comme disposant d'un niveau de protection adéquate.

La Commission européenne et les États-Unis ont conclu un accord imposant des obligations aux sociétés américaines qui se voient communiquer des données à caractère personnel depuis l'Europe. Cet accord se nomme *EU-US Privacy Shield*. Le 12 juillet 2016, la Commission européenne a adopté une décision visant à reconnaître aux principes du *EU-US Privacy Shield* un niveau de protection adéquat. Les entreprises américaines qui ont adhéré à ce mécanisme sont par principe considérées comme assurant un niveau de protection adéquat.

E. Transferts moyennant des garanties appropriées

En l'absence de décision d'adéquation, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu (en vue de compenser l'insuffisance de la protection des données) :

1. des garanties appropriées (en fonction du mécanisme retenu, une autorisation de l'autorité de contrôle peut devoir être obtenue) et
2. à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

   Les garanties appropriées en question peuvent être fournies, sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, par :

1. des règles d'entreprise contraignantes (des « *Binding Corporate Rules* » ou BCR) ;
2. un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics (l'équivalent des « BCR » mais pour les autorités publiques) ;
3. des clauses contractuelles types de protection des données adoptées par la Commission européenne ou par une autorité de contrôle des données personnelles et approuvées par la Commission européenne ;
4. un code de conduite assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées ou
5. un mécanisme de certification assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

Sous réserve de l'autorisation de l'autorité de contrôle compétente cette fois (pour donner son autorisation, l'autorité de contrôle devra appliquer le mécanisme de contrôle de la cohérence visé à l'article 63 du RGPD), les garanties appropriées peuvent aussi être fournies, notamment, au cas par cas, par :

1. l'écriture de clauses contractuelles adéquates entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel situé dans le pays tiers ou l'organisation internationale ou
2. des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées.

Les autorisations accordées par un État membre ou une autorité de contrôle sur le fondement de l'article 26.2, de la directive 95/46/CE demeurent valables jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par ladite autorité de contrôle. De même, les décisions adoptées par la Commission européenne sur le fondement de l'article 26.4, de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par une décision de la Commission.

Voyons maintenant l'une de ces garanties appropriées (les BCR) dans le détail.

F. Les règles d'entreprise contraignantes

1. Conditions

Un groupe de sociétés peut soumettre à son autorité de contrôle compétente un ensemble de dispositions, de règles en matière de protection des données personnelles que le groupe entend suivre et respecter. C'est ce que l'on appelle les règles d'entreprise contraignantes (les « *binding corporate rules* » ou BCR en anglais). L'autorité de contrôle des données personnelles saisie va analyser si cet ensemble de règles respectent les exigences fixées par le RGPD et, si tel est le cas, les approuver conformément au mécanisme de contrôle de la cohérence prévu à l'article 63 du RGPD.

2. Une application pour l'ensemble des sociétés du groupe

Les règles proposées par le groupe et qui deviendront juridiquement contraignantes suite à leur approbation par l'autorité de contrôle devront prévoir que :

1. elles seront appliquées par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, y compris leurs employés ;
2. les personnes concernées ont des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel.

3. Contenu des BCR

Les règles d'entreprise contraignantes devront préciser au moins :

1. la structure et les coordonnées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe et de chacune de leurs entités ;
2. les transferts ou l'ensemble des transferts de données, y compris les catégories de données à caractère personnel, le type de traitement et ses finalités, le type de personnes concernées affectées et le nom du ou des pays tiers en question ;
3. leur nature juridiquement contraignante, tant interne qu'externe ;
4. l'application des principes généraux relatifs à la protection des données, notamment la limitation de la finalité, la minimisation des données, la limitation des durées de conservation des données, la qualité des données, la protection des données dès la conception et la

protection des données par défaut, la base juridique du traitement, le traitement de catégories particulières de données à caractère personnel, les mesures visant à garantir la sécurité des données, ainsi que les exigences en matière de transferts ultérieurs à des organismes qui ne sont pas liés par les règles d'entreprise contraignantes ;

5. les droits des personnes concernées à l'égard du traitement et les moyens d'exercer ces droits y compris le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente et devant les juridictions compétentes des États membres et d'obtenir réparation et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes ;
6. l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un État membre, de l'engagement de sa responsabilité pour toute violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'Union. Le responsable du traitement ou le sous-traitant ne pourra être exonéré, en tout ou en partie, de cette responsabilité que s'il prouve que le fait générateur du dommage n'est pas imputable à l'entité en cause ;
7. la manière dont les informations sur les règles d'entreprise contraignantes sont fournies aux personnes concernées, en plus des informations habituelles sur les droits des personnes concernées ;
8. les missions de tout DPD ou de toute autre personne ou entité chargée de la surveillance du respect des règles d'entreprise contraignantes au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, ainsi que le suivi de la formation et le traitement des réclamations ;
9. les procédures de réclamation ;
10. les mécanismes mis en place au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe pour garantir le contrôle du respect des règles d'entreprise contraignantes. Ces mécanismes prévoient des audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits de la personne concernée. Les résultats de ce contrôle devraient être communiqués à la personne ou au DPD et au conseil d'administration de l'entreprise qui exerce le contrôle du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, et devraient être mis à la disposition de l'autorité de contrôle compétente sur demande ;
11. les mécanismes mis en place pour communiquer et consigner les modifications apportées aux règles et pour communiquer ces modifications à l'autorité de contrôle ;
12. le mécanisme de coopération avec l'autorité de contrôle mis en place pour assurer le respect des règles par toutes les entités du groupe

d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, notamment en mettant à la disposition de l'autorité de contrôle les résultats des contrôles ;

13. les mécanismes permettant de communiquer à l'autorité de contrôle compétente toutes les obligations juridiques auxquelles une entité du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, est soumise dans un pays tiers qui sont susceptibles d'avoir un effet négatif important sur les garanties fournies par les règles d'entreprise contraignantes ;
14. la formation appropriée en matière de protection des données pour le personnel ayant un accès permanent ou régulier aux données à caractère personnel.

La Commission européenne pourra, pour les règles d'entreprise contraignantes, préciser la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent.

G. Transferts ou divulgations non autorisés par le droit de l'Union

Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du RGPD.

H. Quid s'il n'existe aucune décision d'adéquation ni aucune garantie appropriée ?

En l'absence de décision d'adéquation ou de garanties appropriées, y compris des règles d'entreprise contraignantes, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes :

1. la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert

pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées ;

2. le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;
3. le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale ;
4. le transfert est nécessaire pour des motifs importants d'intérêt public (l'intérêt public devra avoir été préalablement reconnu comme tel par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis) ;
5. le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;
6. le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
7. le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce.

   Un transfert réalisé au départ d'un tel registre ne pourra porter sur la totalité des données à caractère personnel ni sur des catégories entières de données à caractère personnel contenues dans le registre. Lorsque le registre est destiné à être consulté par des personnes justifiant d'un intérêt légitime, le transfert n'est effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires.

Notons que les autorités publiques ne pourront pas se baser sur le consentement explicite de la personne concernée ni sur les dérogations liées à la conclusion ou l'exécution d'un contrat pour réaliser (en l'absence de décision d'adéquation et de garanties appropriées) des transferts vers des pays hors de l'Union européenne. Leur champ d'application est donc plus réduit (il leur reste quand même les possibilités vues aux points 4 à 7 ci-dessus).

I. Quid si aucune décision d'adéquation, si aucune garantie appropriée et si aucune des autres possibilités n'existe ?

Lorsqu'un transfert ne peut pas être fondé sur une décision d'adéquation ou sur une garantie appropriée, y compris les dispositions relatives aux règles d'entreprise contraignantes, et qu'aucune des dérogations pour des situations particulières n'est applicable, un transfert vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si (ceci n'est pas applicable aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique) :

1. ce transfert ne revêt pas de caractère répétitif ;
2. ne touche qu'un nombre limité de personnes concernées ;
3. est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée.

De plus, le responsable du traitement devra :

1. avoir préalablement évalué toutes les circonstances entourant le transfert de données et
2. avoir offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel.

Comme d'habitude en la matière (et nous n'insisterons jamais assez sur ce point), le responsable du traitement ou le sous-traitant devra documenter, dans les registres des traitements, l'évaluation qu'il a réalisée ainsi que les garanties appropriées qu'il a prises.

Le responsable du traitement devra aussi informer son autorité de contrôle des données personnel du transfert et fournir aux personnes concernées, les informations habituelles concernant leurs droits et plus spécifiquement que leurs données seront transférées en-dehors de l'Union européenne ou vers une organisation internationale ainsi que des intérêts légitimes impérieux qu'il poursuit.

Dans le cas où la Commission européenne n'a encore pris aucune décision d'adéquation pour un certain pays, le droit de l'Union ou le droit d'un État membre peut, pour des motifs importants d'intérêt public, fixer expressément des limites au transfert de catégories spécifiques de données à caractère personnel vers un pays tiers ou à une organisation internationale. Les États membres devront notifier de telles dispositions à la Commission.

Interprétation restrictive

Ces dérogations ou exceptions risquent de faire l'objet d'une interprétation restrictive par les autorités de contrôle et ne doivent donc être utilisées pour fonder un transfert de données qu'avec prudence, après une analyse approfondie préalable du respect des conditions posées par le règlement. Par ailleurs, puisqu'en l'absence de décision d'adéquation, le droit de l'Union européenne ou d'un État membre peut venir fixer des limites au transfert de certaines catégories spécifiques vers des États non membres ou des organisations internationales, il résulte qu'une vérification de ces hypothèses au cas par cas s'impose, en sus des dérogations précitées *stricto sensu*.

J. Coopération internationale dans le domaine de la protection des données à caractère personnel

La Commission européenne et les autorités de contrôle se sont engagées à prendre, à l'égard des pays tiers et des organisations internationales, les mesures appropriées pour :

1. élaborer des mécanismes de coopération internationale destinés à faciliter l'application effective de la législation relative à la protection des données à caractère personnel ;
2. se prêter mutuellement assistance sur le plan international dans l'application de la législation relative à la protection des données à caractère personnel, y compris par la notification, la transmission des réclamations, l'entraide pour les enquêtes et l'échange d'informations, sous réserve de garanties appropriées pour la protection des données à caractère personnel et d'autres libertés et droits fondamentaux ;
3. associer les parties prenantes intéressées aux discussions et activités visant à développer la coopération internationale dans le domaine de l'application de la législation relative à la protection des données à caractère personnel ;
4. favoriser l'échange et la documentation de la législation et des pratiques en matière de protection des données à caractère personnel, y compris en ce qui concerne les conflits de compétence avec des pays tiers.

K. Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail « Article 29 » a :

1. publié des FAQ relatives aux BCR (uniquement en anglais pour l'instant). Les FAQ ont été revues pour la dernière fois le 7 février 2017 ;
2. adopté un document de travail relatif aux éléments et aux principes qui doivent se retrouver dans des BCR. Le document est uniquement disponible en anglais pour l'instant via le site internet du Groupe de Travail (« *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules* », Réf. WP 256). Ce document est soumis à consultation jusqu'au 17 janvier 2018. La version finale sera publiée par après ;
3. publié un document de travail destiné à procurer de l'aide à la Commission européenne et au Groupe de Travail lorsqu'il s'agit d'évaluer le niveau de protection des pays tiers ou des organisations internationales. Ce document n'est pour l'instant disponible qu'en anglais via le site internet du Groupe de Travail (« *Adequacy Referential (updated)* », Réf. WP 254). Il est soumis à consultation jusqu'au 17 janvier 2018. La version finale sera publiée par après.

Fiche de guidance n° 15
Les sous-traitants sous le RGPD

Article 28 du RGPD

Considérant 81 du RGPD

A. Introduction

L'application du RGPD aura une forte influence sur les relations entre responsables de traitement (le « *data controller* ») et sous-traitants (les « *data processors* »). Un « sous-traitant » est défini comme une personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte d'un responsable du traitement.

Jusque-ici, sous l'empire de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, seul le responsable de traitement répondait auprès de l'autorité de contrôle des données personnelles des manquements à la réglementation. Le sous-traitant était, de ce point de vue, à l'abri des sanctions infligées par les autorités de contrôle.

Dorénavant, le montant maximal des sanctions que pourrait avoir à payer le sous-traitant est identique à celui encouru par le responsable de traitement.

Le Règlement tend en effet à rééquilibrer la relation entre les deux opérateurs en mettant des obligations directement à la charge des sous-traitants et en renforçant leurs obligations contractuelles. Le texte prévoit que les manquements d'un sous-traitant puissent être sanctionnés par les autorités de contrôle. L'objectif est e.a. de rendre responsables les fournisseurs de prestation de *cloud computing* dans leurs activités de stockage de données personnelles.

Il est évident que les sous-traitants n'auront aucune responsabilité tant qu'ils respectent le RGPD et qu'ils ne sortent pas des obligations demandées par le responsable du traitement.

Tentons ici de résumer les obligations des sous-traitants :

1. les sous-traitants (sauf dans certains cas de figure pour les entreprises de moins de 250 salariés) devront tenir un registre des activités de traitement effectuées pour le compte de leurs clients ;
2. dans certains cas, ils devront désigner un délégué à la protection des données (DPD) dans les mêmes conditions qu'un responsable de traitement ;
3. ils ne pourront engager un autre sous-traitant qu'avec l'accord général ou explicite du responsable du traitement.

   Dans ce dernier cas, une obligation d'information pèsera sur le sous-traitant. De plus, les obligations contractuelles que le responsable de traitement aura imposées à son sous-traitant devront être répercutées au sous-traitant de second rang. Par ailleurs, le Règlement prévoit que, vis-à-vis du responsable de traitement, le sous-traitant de premier rang sera responsable de la mauvaise exécution de ses obligations par le sous-traitant de second rang ;
4. dans certaines circonstances, ils devront désigner un représentant s'ils ne sont pas établis dans l'UE.

   Tel sera le cas si le sous-traitant procède alors au traitement des données personnelles concernant des personnes situées dans l'Union européenne et que les opérations de traitement sont liées à l'offre de biens et services ou à la surveillance du comportement de ces personnes ;
5. le sous-traitant sera tenu d'une obligation contractuelle de collaboration avec le responsable du traitement puisqu'il devra l'aider à satisfaire aux demandes formulées par les personnes concernées dans le cadre de l'exercice de leurs droits.

   Les sous-traitants ont véritablement une obligation de conseil auprès des responsables pour le compte desquels ils traitent des données. Ils doivent les aider dans la mise en œuvre de certaines obligations du Règlement (étude d'impact sur la vie privée, notification de violation de données, sécurité, contribution aux audits) ;
6. ils devront coopérer avec les autorités de contrôle des données personnelles ;
7. ils devront implémenter les mesures de sécurité adéquates dès la conception du service ou du produit et, par défaut, mettre en place des mesures permettant de garantir une protection optimale des données ;
8. ils devront prévenir sans délai le responsable du traitement s'ils ont connaissance d'une violation de données à caractère personnel (« *personal data breach* »).

Les précisions du RGPD en matière de transferts transfrontaliers s'appliquent aussi aux sous-traitants. De plus, les règles d'entreprise contraignantes (les « BCR ») pour des sous-traitants sont désormais reconnues officiellement.

Le RGPD prévoit expressément que « si, en violation [du Règlement] un sous-traitant détermine les finalités et les moyens du traitement de données, il est considéré comme un responsable de traitement pour ce traitement ». Cette hypothèse trouverait à s'appliquer lorsque le sous-traitant, en violation du contrat conclu avec le responsable de traitement, réutiliserait les données personnelles qui lui sont confiées pour mettre en œuvre un traitement dont il est seul à définir la finalité et les moyens. En pareil cas, le sous-traitant engagerait sa responsabilité vis-à-vis du responsable de traitement mais il encourrait également des sanctions pénales et administratives.

B. Contenu minimum d'un contrat avec un sous-traitant

Sans qu'il s'agisse d'une nouveauté (certaines des exigences du Règlement étaient déjà insérées dans les contrats par les praticiens), le sous-traitant devra présenter des garanties suffisantes (connaissances du domaine dans lequel il intervient, fiabilité et ressources notamment) de mise en œuvre de mesures techniques et organisationnelles pour que le traitement soit conforme au Règlement et garantisse la protection des droits de la personne concernée.

Ces garanties constitueront d'ailleurs un critère que les responsables de traitement devront prendre en compte lorsqu'ils devront sélectionner un nouveau sous-traitant (« Mon futur sous-traitant a-t-il au moins le même niveau de protection/sécurité que moi ? »).

Cette exigence pourra, par exemple, être satisfaite lorsque le sous-traitant appliquera un code de conduite approuvé par une autorité de contrôle. Le responsable de traitement devra utilement demander au prestataire pressenti sa politique en matière de protection des données personnelles et procéder à des vérifications récurrentes (des audits).

Le contrat (conclu par écrit, y compris sous forme électronique) avec le sous-traitant devra dorénavant obligatoirement préciser que le sous-traitant :

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union européenne ou du droit de l'État membre auquel le sous-traitant est soumis.

   Dans ce cas, le sous-traitant devra informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public. De ce point de vue, le cahier des charges pourrait

être un outil. Les instructions pourront également figurer en annexe du contrat ;

b) veille à ce que ses personnes autorisées à traiter les données à caractère personnel (salariés, consultants notamment) s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

c) prend toutes les mesures de sécurité requises en vertu de l'article 32 du RGPD.

Il devra donc mettre en œuvre des mesures techniques et organisationnelles de nature à protéger les données personnelles qu'il traitera pour le compte du responsable de traitement (chiffrement, anonymisation, etc.). Cette obligation devra être contractualisée ;

d) respecte certaines conditions lorsqu'il entend recruter un autre sous-traitant (ces conditions seront généralement spécifiées dans le contrat avec le responsable du traitement) ;

e) tenant compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées et dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes des personnes concernées ;

f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD (sécurité des données, notification en cas de violation des données et analyse d'impact relative à la protection des données), compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;

g) au terme de la prestation de services relatifs au traitement et selon les dispositions du contrat le liant au responsable du traitement, il devra ou supprimer toutes les données à caractère personnel mises à sa disposition par ledit responsable ou bien les lui renvoyer après avoir détruit les copies existantes, à moins toutefois que le droit de l'Union ou son droit national n'exige la conservation de ces données à caractère personnel ;

h) met à la disposition du responsable du traitement et de manière continue toutes les informations nécessaires pour lui démontrer qu'il respecte bien ses obligations.

Le sous-traitant devra permettre la réalisation d'audits exigées par le responsable du traitement et contribuer de bonne foi à ces audits. Le sous-traitant devra agir de manière proactive et informer immédiatement le responsable du traitement si, selon lui, une de ses instructions constitue une violation du Règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

C. Les précautions que les sous-traitants doivent prendre en compte pour intégrer les nouvelles exigences du RGPD

Le statut de « sous-traitant » n'est pas nouveau. Toutefois, on vient de le voir, son statut est désormais plus exigeant.

Le responsable du traitement ne peut pas choisir n'importe quel sous-traitant. Il devra choisir un sous-traitant qui présente « des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement (le RGPD) et garantisse la protection des droits de la personne concernée ».

La protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel exige en effet l'adoption tant par le responsable du traitement que le sous-traitant de l'implémentation de mesures techniques et organisationnelles appropriées. Ces mesures devront être efficaces et garantir que les exigences du RGPD sont respectées.

Un sous-traitant dispose d'un mandat de traitement des données personnelles, défini par le responsable du traitement et agira uniquement sur instruction de celui-ci.

Le mandat sera formalisé par l'intermédiaire des contrats qui lient le sous-traitant à ses clients. Ainsi, une mise à jour active et continuelle des modèles de contrats en intégrant directement les clauses obligatoires décrites à l'article 28 du RGPD permet d'être conforme contractuellement. Afin d'établir les rôles et responsabilités en matière de protection des données personnelles, une politique et une matrice de responsabilité type peuvent également être établies.

D. Le sous-traitant doit se positionner comme partenaire de confiance

Le RGPD insiste sur les devoirs du sous-traitant :

- un devoir de conseil, notamment sur les sujets de sécurité ;
- un devoir d'assistance en cas de demande des personnes concernées ;
- un devoir de coopération, par exemple en cas de contrôle d'une autorité de contrôle des données personnelle.

Des devoirs qui nécessitent pour le sous-traitant de se positionner comme partenaire de confiance pour ses clients. Une confiance et une coopération mutuelles d'autant plus indispensables que les sanctions sont désormais partagées, le sous-traitant pouvant être contrôlé et sanctionné par l'autorité de

contrôle des données personnelles au même titre que l'est aujourd'hui le responsable du traitement.

E. Le sous-traitant, un maillon d'une chaîne de conformité

Le sous-traitant occupe un maillon clé d'une chaîne de conformité et interagit avec différents acteurs. Il est parfois en relation contractuelle directe avec le responsable du traitement, et parfois avec le sous-traitant d'un responsable de traitement (un éditeur SaaS sous contrat avec un hébergeur par exemple). La conformité au RGPD du sous-traitant est une condition essentielle pour assurer la conformité de la chaîne globale de sous-traitance.

Mais elle n'est pas suffisante : chaque maillon devra être en capacité de démontrer sa conformité. Via le processus de gestion des fournisseurs, il est nécessaire de garantir que les prestataires, aussi bien en amont qu'en aval de la chaîne de sous-traitance, répondent aux exigences.

Le RGPD contient des suggestions en matière de sécurité et ce que pourraient être les mesures à prendre pour faire face aux risques :

1. pseudonymiser le plus tôt possible les données voire les chiffrer ;
2. assurer la confidentialité, l'intégrité, la disponibilité et la résistance des systèmes internes et des services qui traitent des données à caractère personnel ;
3. permettre de restaurer rapidement la disponibilité des données ainsi que leur accès dans le cas où un incident physique ou technique s'est produit ;
4. procéder régulièrement à des tests et des analyses afin d'évaluer l'effectivité des mesures techniques et organisationnelles qui ont été prises afin d'assurer la sécurité des traitements.

Le fait d'adhérer à un code de conduite ou de disposer d'une certification adéquate pourrait aussi permettre à la société de démontrer sa conformité au RGPD.

F. Le ISMS (*Information Security Management System*), un appui incontournable

Le ISMS (ou SMSI, Système de Management de la Sécurité de l'Information) est un outil incontournable dans le processus de mise en conformité au RGPD. Plus il est mature, c'est-à-dire plus il s'est enrichi de nouveaux référentiels

tels que ISO 27002, PCI-DSS ou encore le formulaire P6 de l'Agrément HDS en France, moins il sera complexe de répondre aux exigences du RGPD.

En s'appuyant sur l'organisation, les procédures, et les mesures de sécurité existantes, puis en les enrichissant, notamment via les contrôles complémentaires du référentiel ISO 27018 relatif à la sécurité des données personnelles dans le cloud, le sous-traitant peut faire converger les deux démarches dans un ensemble cohérent.

Ainsi, la désignation du DPD, la sensibilisation des équipes internes à la protection des données personnelles et aux nouveaux outils à intégrer font parties des étapes indispensables pour intégrer le RGPD en toute sérénité.

Aujourd'hui, les sous-traitants s'appuient principalement sur les directives du Groupe de Travail « Article 29 » pour les premiers travaux de mise en conformité. Ces divers éléments ne seront pas les seuls à prendre en compte. Ainsi, il faut s'attendre à de nouvelles directives du Groupe de Travail « Article 29 », à la déclinaison du RGPD en actes délégués, ou encore à la révision des lois nationales en matière de protection des données à caractère personnel et à leurs mesures d'application/d'exécution.

Afin d'anticiper ces éventuels changements, il est utile de rester en veille permanente afin d'ajuster les travaux réalisés, en cours et à venir.

Fiche de guidance n° 16
Les modalités d'exercice des droits des personnes concernées

Article 12 du RGPD

Considérants 58 & 61 du RGPD

Introduction

Dans le cadre du RGPD (comme déjà dans le cadre de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données), les personnes concernées ont certains droits leur permettant de contrôler les activités du responsable du traitement. Il est indispensable que les personnes concernées soient informées de leurs droits lorsque le responsable du traitement collecte et obtient leurs données.

L'article 12 du RGPD précise les modalités d'exercice des droits des personnes concernées (et corrélativement, des obligations des responsables du traitement).

A. Langage des réponses (droit à la compréhension ou principe de transparence)

Les explications et réponses du responsable du traitement doivent être concises, transparentes, compréhensibles et aisément accessibles en des termes clairs, intelligibles et simples. Il est conseillé au responsable de traitement de ne pas utiliser de jargon scientifique ou juridique mais d'accompagner si possible

son message d'éléments visuels. Tout ceci fait partie du grand « principe de transparence ».

Ce principe de transparence n'est pas limité à l'information des personnes puisque qu'il impose au responsable de traitement de faciliter l'exercice par les personnes des droits qui leur sont reconnus.

Les informations à fournir en vertu des articles 13 et 14 (« Information et accès aux données à caractère personnel ») du RGPD pourront être fournies accompagnées (pas remplacées) par des icônes normalisées ceci afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu. Lorsque les icônes sont présentées par voie électronique, elles devront pouvoir être lues par une machine.

La Commission européenne doit déterminer :

1. quelles seront les informations qui pourront être présentées sous la forme d'icônes (toutes ne pourront donc pas être présentées sous forme d'icônes) ;
2. ainsi que les procédures régissant la fourniture d'icônes normalisées.

À ce jour, cet acte délégué de la Commission européenne n'a pas encore été pris.

B. Canal de communication

Les informations/réponses devront être fournies par écrit.

Les informations seront fournies par voie électronique (par exemple, via mail/un site web) lorsque :

1. c'est approprié ou possible ;
2. la personne concernée envoi une demande sous une forme électronique ;
3. cette demande exige une réponse sous format électronique également.

A contrario, la personne concernée peut tout à fait, électroniquement, demander que les informations lui soient fournies autrement (sous format papier par exemple).

Les réponses pourront également être fournies oralement. Toutefois, afin d'éviter toute fraude :

1. il faudra que la personne concernée en ait fait la demande. Cela ne pourra donc pas être fait d'initiative par le responsable du traitement ;
2. l'identité de la personne concernée devra être démontrée par d'autres moyens afin que l'on soit bien sûr que c'est elle qui a demandé des explications orales.

Le responsable du traitement doit répondre et même tout faire pour faciliter l'exercice des droits de la personne concernée. Ce n'est que lorsqu'il n'a pas pu identifier la personne concernée qu'il est autorisé à ne pas répondre. Il devra toutefois réagir et prévenir cette personne qu'il n'a pas pu l'identifier.

Si le responsable du traitement a des doutes raisonnables quant à l'identité de la personne concernée, il peut exiger que la personne concernée lui fournisse des informations supplémentaires pour confirmer son identité.

C. Délai

Le responsable du traitement doit répondre à la demande de la personne concernée dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande.

Une revue voire une adaptation des procédures de traitement des courriers entrant, qu'ils soient postaux ou électroniques, de chaque société devra donc être mise en œuvre afin que le responsable de traitement s'assure que les délais stricts qui lui sont impartis sont bien respectés. Il est plus que nécessaire qu'une procédure de gestion de ce type de demande soit mis en place.

Le délai d'un mois pourra être prolongé de deux mois (on passe donc d'un mois à trois mois) :

1. si la demande est complexe et
2. si le responsable du traitement a reçu beaucoup de demandes.

Le responsable devra informer dans le délai d'un mois la personne concernée :

1. de la prolongation du délai et
2. des motifs du report.

Si le responsable du traitement n'entend pas donner suite à la demande de la personne concernée :

1. il devra informer la personne concernée de ce fait ;
2. il devra l'informer dans le délai d'un mois qui court à compter de la réception de la demande ;
3. il devra préciser les motifs de son refus et
4. ajouter que la personne concernée peut introduire une réclamation auprès de l'autorité de contrôle nationale.

D. Coût

Le responsable du traitement ne peut exiger aucun paiement pour :

1. fournir les informations à la personne concernée ;
2. avoir pris les mesures internes qui étaient nécessaires afin d'être en conformité avec les articles 15 à 22 et 34 du RGPD.

Toutefois, lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives notamment en raison de leur caractère répétitif, le responsable du traitement peut :

1. exiger un paiement ;
2. refuser de donner suite à ces demandes.

Ce sera au responsable du traitement à démontrer que la demande était infondée ou excessive.

E. Les Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail « Article 29 » a publié des Lignes directrices en rapport avec le principe de transparence. Ces Lignes directrices sont soumises à consultation jusqu'au 23 janvier 2018. La version finale du document sera adoptée et publiée plus tard (« *Guidelines on transparency under Regulation* 2016/679 », Ref. WP 260).

F. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 3 : Les principes généraux de protection des données*
- *Fiche de guidance n° 4 : L' « accountability »*
- *Fiche de guidance n° 6 : Le consentement*
- *Fiche de guidance n° 18 : Droit 1 : Le droit d'information des personnes concernées*

Fiche de guidance n° 17
Les huit droits des personnes concernées

Articles 13 à 22 du RGPD

Dans le cadre du RGPD et par rapport à la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les personnes concernées ont vu leurs droits renforcés et augmentés.

Elles disposent dorénavant des droits suivants (elles doivent en être informées au moment où le responsable du traitement collecte et obtient leurs données personnelles) :

1. le droit d'obtenir de la part du responsable de traitement certaines informations. Ces informations doivent être fournies par le responsable du traitement au moment de la collecte des données à caractère personnel (notons que si le responsable du traitement obtient les données de quelqu'un d'autre que la personne concernée, le responsable du traitement a aussi l'obligation de fournir des informations à la personne concernée) ;
2. le droit d'accéder aux données personnelles qui la concerne et qui sont détenues par le responsable du traitement et d'en obtenir copie ;
3. le droit que le responsable du traitement corrige des données qui les concernent et qui seraient erronées ;
4. le droit d'obtenir, sous certaines conditions, du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant ;
5. le droit d'obtenir, sous certaines conditions, la limitation (= la suspension) d'un traitement ;
6. le droit à la portabilité de leurs données (ici aussi sous certaines conditions) ;

7. le droit de s'opposer, sous certaines conditions, à des traitements et le droit de s'opposer à tout moment au traitement de leurs données à caractère personnel les concernant à des fins de prospection telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection ;
8. le droit, dans certaines hypothèses, à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques les concernant ou les affectant de manière significative.

Ces droits sont détaillés dans les Fiches de guidance qui suivent.

Fiche de guidance n° 18
Droit 1 : Le droit d'information des personnes concernées

Articles 13 et 14 du RGPD

Considérants 39, 58 à 63 du RGPD

A. Introduction

Avant de commencer ses activités de traitement, le responsable du traitement se doit d'informer les personnes concernées sur un certain nombre de points.

Comme pour la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (articles 10 et 11), deux hypothèses sont ici à envisager :

- soit les données sont collectées par le responsable du traitement auprès de la personne concernée elle-même (art. 13 du RGPD) ;
- soit les données n'ont pas été collectées auprès de la personne concernée (art. 14 du RGPD).

Les informations à fournir par le responsable du traitement varient selon qu'il s'agit de la première hypothèse ou de la seconde.

B. Première hypothèse : les données ont été collectées auprès de la personne concernée

1. Principe de transparence

Dans ce cas, au moment où les données sont obtenues, le responsable du traitement doit fournir à la personne concernée une série d'informations :

1. l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement.

   Il est conseillé de mentionner différents moyens de contacter le responsable du traitement (numéro de téléphone, email, adresse physique) ;
2. le cas échéant, les coordonnées du délégué à la protection des données (le DPD) (par forcément son identité mais un moyen de le contacter même s'il s'agit d'une adresse email générique comme privacy@société.be) ;
3. les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;
4. lorsque le traitement est fondé sur l'article 6.1.f du RGPD, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

   Le responsable du traitement devrait aussi indiquer l'analyse des intérêts (les siens versus ceux des personnes concernées à ne pas voir leurs données collectées et traitées) qu'il doit avoir réalisée pour pouvoir justifier le choix de cette base juridique (exercice difficile s'il en est car il va requérir un véritable travail d'introspection de la part des responsables du traitement) ;
5. les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent.

   Les destinataires sont les personnes physiques ou morales (qu'il s'agisse ou non d'un tiers) qui vont recevoir les données personnelles ou y avoir accès. Il est conseillé de les nommer. Si le responsable du traitement décide de mentionner uniquement des catégories de destinataires (aussi précises que possible dès lors), il devra être capable de dire pourquoi il a choisi une telle approche ;
6. le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission européenne ou, dans le cas des transferts visés à l'article 46, 47 ou à l'article 49.1, deuxième alinéa du RGPD, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

Le Groupe de Travail « Article 29 » conseille de mentionner explicitement tous les pays tiers vers lesquels les données peuvent être transférées.

En plus des informations précédentes, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes nécessaires pour garantir un traitement équitable et transparent :

1. la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée.

   Ici aussi, le principe de loyauté impose aux responsables du traitement d'être aussi précis que possible afin de permettre aux personnes concernées de comprendre, en fonction de leur situation personnelle, quelle va être la période de rétention de leurs données pour telles finalités et/ou des activités de traitement en ce compris, si c'est approprié, les périodes d'archivage ;

2. l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, une limitation du traitement relatif à la personne concernée ou du droit de s'opposer au traitement et du droit à la portabilité des données.

   Les informations devraient reprendre un résumé des droits et de ce qu'ils impliquent et de la manière dont les personnes concernées peuvent les exercer auprès du responsable du traitement ;

3. l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22.1 et 22.4 du RGPD, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ;

4. lorsque le traitement est fondé sur le consentement de la personne concernée (explicite) (article 6.1.a ou article 9.2.a du RGPD), l'existence du droit de retirer ce consentement à tout moment, comment peut se réaliser ce retrait. Le retrait doit se réaliser d'une manière aussi facile que la fourniture du consentement ;

5. le droit d'introduire une réclamation auprès d'une autorité de contrôle ;

6. des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel, si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel.

   Le responsable du traitement devra aussi clairement expliquer quelles sont les conséquences éventuelles de la non-fourniture par la personne concernée de ses données.

Par exemple, sur un formulaire en ligne, il devrait être clairement indiqué quels champs sont obligatoires et lesquels ne le sont pas et quelles sont les conséquences si la personne concernée ne fournit pas les informations requises obligatoirement.

Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement devra fournir au préalable à la personne concernée des informations au sujet de cette autre finalité.

Il découle de ce qui précède que lorsque le traitement se déroule en ligne et donc immédiatement, le responsable du traitement devra fournir toutes les informations en une fois à la personne concernée.

Le droit à l'information ne s'applique pas lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations. Ce sera au responsable de traitement à prouver, en cas de litige, que la personne concernée disposait déjà des informations.

2. La raison d'être de la séparation des 12 catégories d'information

On peut se poser la question de savoir *pourquoi* l'article 13 sépare en deux les informations à donner à la personne concernée (alors que la proposition de Règlement de la Commission européenne de 2012 ne contenait qu'une seule liste en continu des informations à fournir).

La compréhension se trouve dans la lecture attentive du début du § 1 et du § 2.

Le § 1 commence en disant que c'est « au moment où les données sont collectées » qu'il faut fournir le premier set d'informations (que l'on pourrait qualifier d'informations de base ou d'informations à fournir au minimum). Le § 2 commence lui en disant qu'en plus des informations précédentes, le responsable du traitement doit fournir à la personne concernée ce second set d'informations mais uniquement « au moment où les données à caractère personnel sont obtenues » et ceci pour garantir un traitement équitable et transparent.

Prenons l'exemple du monde des assurances afin de mieux comprendre.

Un contrat d'assurance est conclu en deux étapes. Le client se rend chez son courtier. Ce dernier analyse les besoins et exigences du client. Sur cette base, il lui propose le contrat qu'il lui semble approprié. Le courtier remplit une proposition d'assurance qu'il renvoie à la compagnie d'assurances. Sur la base de ce document, la compagnie va décider si oui ou non elle décide de conclure le contrat avec le client. Si elle décide de conclure le contrat avec le client, elle va lui envoyer les conditions particulières et les conditions générales liées à ces conditions particulières.

La proposition d'assurance doit contenir le premier set d'informations (les informations de base). Car c'est à ce moment-là que le courtier collecte les données à caractère personnel du client. Le second set d'informations sera repris dans les conditions générales que la compagnie enverra au futur client après qu'elle ait obtenue les données personnelles de celui-ci de la part du courtier. Généralement, les conditions générales reprendront tant le premier que le second set d'informations de l'article 13 du RGPD.

C. Seconde hypothèse : les données à caractère personnel n'ont pas été collectées auprès de la personne concernée

1. Principe de transparence

Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable du traitement devra fournir à la personne concernée toutes les informations suivantes :

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;

b) le cas échéant, les coordonnées du délégué à la protection des données ;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;

d) les catégories de données à caractère personnel concernées ;

e) le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel ;

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49.1, deuxième alinéa du RGPD, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

En plus de ces informations, le responsable du traitement devra fournir à la personne concernée les informations suivantes nécessaires pour garantir un traitement équitable et transparent à l'égard de la personne concernée :

a) la durée pendant laquelle les données à caractère personnel seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

b) lorsque le traitement est fondé sur l'article 6.1.f du RGPD, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;

c) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ainsi que du droit de s'opposer au traitement et du droit à la portabilité des données ;

d) lorsque le traitement est fondé sur l'article 6.1.a ou sur l'article 9.2.a du RGPD, l'existence du droit de retirer le consentement à tout moment.

Que le responsable se rassure, ce retrait ne portera pas atteinte à la licéité des traitements qui étaient fondés sur le consentement et qui avaient été effectués avant le retrait du consentement ;

e) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;

f) la source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public ;

g) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22.1 et 22.4 du RGPD et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

2. Délai de communication : un mois

Dans le cas où les données n'ont pas été collectées auprès de la personne concernée mais auprès d'un tiers, le responsable du traitement dispose d'un certain délai pour communiquer à la personne les informations que nous avons énumérées plus haut.

En effet, il devra fournir ces informations aux personnes concernées :

a) dans un délai raisonnable après avoir obtenu les données à caractère personnel. Ce délai ne pourra pas dépasser un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées ;

b) si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne ;

c) s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

Selon le Groupe de Travail « Article 29 » (dans leur document WP 260, p. 14), la fourniture des informations aux personnes concernées devra obligatoirement être réalisée dans le délai d'un mois du point a). Ce n'est que si le

responsable du traitement va utiliser les données pour communiquer avec les personnes concernées (point b) ou s'il envisage de communiquer les données à un autre destinataire (point c) que la communication peut (et devra) se réaliser avant.

Autrement dit, si le responsable du traitement envisage d'utiliser les données pour communiquer avec les personnes concernées mais dans un délai supérieur à un mois après avoir obtenu les données, il devra quand même fournir les informations de l'article 14 du RGPD dans le délai d'un mois. Parallèlement, le responsable devra quand même informer les personnes concernées dans le délai d'un mois s'il envisage de communiquer les données collectées à un autre destinataires mais ultérieurement au délai d'un mois.

Nous conseillons dès lors aux responsables du traitement, dans le cas d'une collecte de données indirectes, de toujours bien tenir à l'œil ce délai très court d'un mois.

Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité.

3. Pas d'obligation de fournir les informations

Dans le cas où les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement est parfois dispensé de communiquer les diverses informations de l'article 14 du RGPD à ladite personne concernée. Ces hypothèses sont d'interprétation restrictive et ce sera toujours au responsable du traitement à prouver, en cas de contestation, qu'il pouvoir bien bénéficier de l'exception.

À nouveau, si le responsable du traitement veut se baser sur une des exceptions pour ne pas informer la personne concernée, nous lui conseillons de documenter sa décision dans le cas d'un futur contrôle ou d'une possible question.

Le responsable est dispensé de fournir les informations lorsque et dans la mesure où :

a) la personne concernée dispose déjà de ces informations ;

b) la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés ou dans la mesure où l'obligation d'information est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement envisagé par le responsable.

   Dans pareilles situations, le responsable du traitement devra prendre des mesures appropriées pour protéger les droits et libertés ainsi que

les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles via son site web par exemple ;

c) l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union européenne ou le droit de l'État membre auquel le responsable du traitement est soumis.

La législation en question devra prévoir des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée ;

d) les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union européenne ou le droit des États membre, y compris une obligation légale de secret professionnel.

Nous recommandons aux responsables de traitement de, dès à présent, cataloguer les endroits et les moments où ils collectent des informations à caractère personnel.

Ces supports peuvent être multiples : formulaires de collecte de données (papier, en ligne) ; documents (pré-) contractuels (contrat avec les fournisseurs, contrat de travail, etc.) ; « politique de protection des données » ou « privacy policy » d'un site web ; etc.

La société devrait aussi écrire et confectionner une bibliothèque des différentes hypothèses où elle capte des données personnelles. Il s'agirait de réaliser une bibliothèque de mentions d'information type, qui tiendrait compte des divers types de traitement pouvant être mis en œuvre au sein de l'entité, des finalités poursuivies, des caractéristiques de ces traitements, des modalités de collecte des données, etc. afin de disposer de modèle harmonisés et réutilisables.

Et, enfin, de formaliser un process interne imposant, pour tout nouveau projet nécessitant une collecte / utilisation de données à caractère personnel, de vérifier l'existence, les modalités et le contenu de l'information des personnes concernées en se basant sur les clauses et informations type qui sont stockées dans la bibliothèque « privacy » de la société.

D. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

➠ *Fiche de guidance n° 16 : Les modalités d'exercice des droits des personnes concernées*

Fiche de guidance n° 19
Droit 2 : Le droit d'accès de la personne concernée

Article 15 du RGPD

Considérants 63, 64 & 73 du RGPD

A. Introduction

Même si ce droit était déjà prévu dans la Directive de 1995, il est dorénavant mieux encadré et précisé.

Le droit d'accès (« *Subject Access Request* » en anglais ou « S.A.R. ») est un droit de questionnement de la personne concernée sur l'existence ou non d'informations la concernant dans un traitement de données. Pour beaucoup, il s'agit de l'un des droits les plus importants des personnes concernées. Ce questionnement porte sur le droit de savoir si des données la concernant font effectivement l'objet d'un traitement par un responsable de traitement et, dans l'affirmative, quelles sont les données précisément traitées et quelles sont leur origine.

Avant d'avoir accès à ses données personnelles, la personne concernée doit évidemment questionner le responsable du traitement afin de savoir si oui ou non ce responsable traite des données à caractère personnel la concernant.

Ce n'est que si la réponse est positive que la personne concernée pourra avoir accès aux données à caractère personnel qui la concerne et qui sont traitées par ledit responsable du traitement, obtenir du responsable du traitement certaines informations et, le cas échéant, une copie des données à caractère personnel faisant l'objet d'un traitement.

Ce droit permet à la personne concernée d'être au courant du traitement et de vérifier sa légalité.

Lorsque la personne concernée présente sa demande par voie électronique, les informations devront lui être fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande une réponse papier.

B. Contenu du droit d'accès

Quelles sont les informations que la personne concernée peut obtenir ?

1. les finalités du traitement ;
2. les catégories de données à caractère personnel concernées ;
3. les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales ;
4. lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
5. l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement ;
6. le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
7. lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ;
8. l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22.1 et 22.4 du RGPD, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées ou adaptées prises par le responsable du traitement, en vertu des article 46, 47 et 49.1, deuxième alinéa du RGPD, en ce qui concerne ce transfert.

Il est très important pour les sociétés de bien savoir gérer les demandes d'accès des personnes concernées et d'y répondre en respectant toutes les exigences du RGPD (voir l'article 12 du RGPD pour les modalités et surtout le délai). Des arriérés trop importants seront le signe, pour les autorités de contrôle des données personnelles, de problèmes d'organisation pour une société en matière de protection des données à caractère personnel.

Le RGPD a raccourci le délai de 40 jours de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données à un mois.

La demande doit aussi être traitée gratuitement. En effet, le responsable du traitement ne peut exiger le paiement de frais par rapport à sa gestion de

la demande de la personne concernée. Il pourra exiger des frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée.

Le responsable du traitement est totalement responsable de la conformité au RGPD et devra s'assurer que son sous-traitant (son « *Data Processor* ») est capable de fournir toutes les informations nécessaires afin de permettre que lui puisse répondre aux personnes concernées dans le mois. Il faudra dorénavant que les contrats avec les sous-traitants contiennent des SLA (« *Service Level Agreement* ») sur les temps de réponse voulus par les responsables de traitement.

Il serait bon que chaque responsable du traitement implémente assez vite une procédure interne afin d'être sûr qu'il puisse répondre dans le mois (process IT adéquats, personnel informé et formé en conséquence via des formations sur ce sujet). N'oublions pas que le responsable de traitement devra répondre aux personnes concernées de la manière choisie par ces dernières et non pas uniquement via le canal de communication qu'ils auraient mis à la disposition des personnes concernées.

Une des suggestions pour les responsables de traitement pour satisfaire aux futures demandes des personnes concernées est de mettre en place un outil électronique (semi-)automatique (un « *Privacy Dashboard* ») pour permettre aux personnes concernées de pouvoir télécharger directement elles-mêmes les données personnelles qui les concernent via cet outil.

Toutefois, il s'agirait quand même pour les responsables de traitement de garder un œil sur cet outil. En effet, l'exercice du droit d'accès ne peut nuire aux droits et libertés des tiers. Cela pourrait inclure la protection des secrets d'affaires, des droits de propriété intellectuelle, etc. Dès lors, il faudrait que les responsables de traitement mettent en place une façon de vérifier l'identité des personnes concernées ainsi que le contenu des données que les personnes concernées vont télécharger afin de voir s'il n'existe pas des restrictions légales quant à la mise à disposition de certaines données.

Une des principales difficultés pratiques pour le responsable de traitement est de pouvoir déterminer quelles sont les données qu'il faut examiner afin d'être en conformité avec le RGPD. Une cartographie de ce que le responsable possède comme données personnelles et de l'endroit où elles sont situées est plus que nécessaire.

Par exemple, les catégories de données suivantes devraient être examinées :

1. les informations détenues dans des banques de données électroniques ;
2. les enregistrements des correspondances que ce soient des correspondances « physiques » ou des emails, etc. ;
3. les enregistrements détenus dans un système manuel du moment que le système est hautement structuré et permette de retrouver facilement l'information ;

4. les données de santé, d'éducation, sur des services sociaux ;
5. toutes les informations détenues par une autorité publique ;
6. les enregistrements vidéos et audios ;
7. les enregistrements d'activités de traitement effectués sur des informations personnelles d'individus ;
8. les archives et les back-ups.

C. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

➠ *Fiche de guidance n° 16 : Les modalités d'exercice des droits des personnes concernées*

Fiche de guidance n° 20
Droit 3 : Le droit de rectification de la personne concernée

Article 16 du RGPD

Considérants 59 & 156 du RGPD

A. Contenu

La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes.

De plus, compte tenu des finalités du traitement, la personne a le droit d'obtenir que les données à caractère personnel incomplètes la concernant soient complétées, y compris en fournissant une déclaration complémentaire.

La différence entre les deux possibilités est subtile.

La deuxième possibilité vise le fait que « compte tenu des finalités du traitement », le responsable du traitement refuse de compléter directement les données incomplètes dans sa banque de données mais accepte uniquement d'y ajouter une déclaration de la personne concernée en question, déclaration visant à préciser que ses données sont incomplètes et qu'il faut tenir compte en plus de tel ou tel élément mentionné(s) dans une déclaration complémentaire.

L'article 12.b de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données précisait déjà que : « Les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement : (…) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données ».

On le voit, le RGPD a précisé ce droit qui devrait permettre aux personnes concernées d'exercer plus de contrôle sur l'utilisation de leurs données personnelles.

B. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 16 : Les modalités d'exercice des droits des personnes concernées*
- *Fiche de guidance n° 21 : Droit 4 : Le droit à l'« oubli » de la personne concernée*

Fiche de guidance n° 21
Droit 4 : Le droit à l' « oubli » de la personne concernée

Article 17 du RGPD

Considérants 65, 66 & 156 du RGPD

A. Introduction

Notons tout d'abord que l'expression « droit à l'oubli » ne se retrouve qu'au titre de l'article et que les titres n'ont pas de valeur juridique dans le RGPD. Dès lors, « ce droit à l'oubli » n'en est pas vraiment un et sa mention a surtout une valeur purement symbolique.

Grâce à ce droit, la personne concernée peut exiger, mais sous certaines conditions, du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant. Le responsable du traitement ne devra pas rester inactif mais effacer ces données dans les meilleurs délais également.

Autrement dit, les utilisateurs pourront demander aux entreprises d'effacer leurs données personnelles, d'arrêter leur diffusion et d'empêcher ainsi les tiers d'y accéder.

Les entreprises des secteurs privé et public devront prouver que les données sont effacées en toute sécurité et ce conformément aux nouvelles lignes directrices.

B. Ce droit n'est pas absolu (partie 1)

Comme pour la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ce droit n'est pas général. Il ne pourra s'appliquer que pour des motifs limitativement énumérés, ce qui va en diminuer grandement la portée.

En effet, la personne concernée ne pourra exercer le droit à l'effacement de ses données à caractère personnel détenues par un responsable de traitement que si l'un des six motifs suivants s'applique :

1. les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées (il s'agit du pendant de l'obligation du responsable de traitement de ne garder les données que le temps nécessaire à leur traitement) ;
2. la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6.1.a ou à l'article 9.2.a du RGPD et il n'existe pas d'autre fondement juridique au traitement ;
3. la personne concernée s'oppose :
   a) pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6.1.e du RGPD (« traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ») ou 6.1.f du RGPD (« traitement nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers »), y compris un profilage fondé sur ces dispositions, et il n'existe pas de motif légitime impérieux pour le responsable du traitement pour quand même effectuer ledit traitement,
   b) au traitement des données à caractère personnel la concernant à des fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection ;
4. les données à caractère personnel ont fait l'objet d'un traitement illicite autrement dit lorsque le traitement a été réalisé alors que le responsable de traitement n'avait aucune des bases légales de l'article 6 du RGPD pour le faire ;
5. les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union européenne ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
6. les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8.1 du RGPD (enfant).

C. Comment supprimer définitivement les données ?

Traditionnellement, se débarrasser des données des supports de stockage était limité aux disques durs, aux PC et aux ordinateurs portables une fois qu'ils

ont atteint la fin de leur durée de vie. Dans un monde de plus en plus « virtuel », le besoin d'effacer les données en toute sécurité a dépassé le périphérique de stockage physique.

1. Les différents types d'effacements

Pour effacer intégralement et de façon sécurisée des périphériques pour qu'ils soient réutilisés, revendus ou recyclés, une solution d'effacement de données sécurisée s'impose.

Si nécessaire, il faut que la solution choisie permette de traiter de façon efficace les disques durs, les disques SSD et les serveurs ainsi que toutes les mémoires des téléphones mobiles et des Data Center qui contiennent une énorme quantité de données.

Il faudra non seulement effacer l'index mais aussi écraser de façon sécurisée toutes les données contenues sur le disque, rendant la reconstruction des données impossible.

2. Prouver que les données ont bien été effacées

Outre le processus d'effacement, la société devra prouver que les données ont été effacées, ceci alors que les systèmes informatiques ont toujours été construits pour empêcher toute perte de donnée. Dès lors, la solution choisie devra générer des rapports exhaustifs attestant de la réussite de l'effacement. Ces rapports infaillibles et vérifiables constitueront un maillon essentiel pour satisfaire les impératifs réglementaires, de conformité et d'audit juridique. Ils fourniront des informations cruciales pour le processus d'audit, telles que :

- l'état du matériel ;
- les numéros d'inventaire et de série correspondants ;
- la personne ayant réalisé l'effacement et la méthode utilisée.

D. Avantages pour une entreprise à effacer les données

Il existe plusieurs avantages pour une entreprise à mettre en place une politique d'effacement des données, et pas seulement en raison de la nouvelle orientation de la législation européenne :

1. *Coût* – Le stockage de données physique et virtuel coûte cher. Les organisations peuvent réaliser des économies importantes dans leur

budget informatique en réattribuant ou en revendant le stockage au lieu de le détruire physiquement. Des systèmes de stockage de données complexes sont coûteux à remplacer. Par conséquent, il est plus logique d'effacer en toute sécurité les données sur un lecteur ou un système virtuel en utilisant un logiciel, plutôt que d'utiliser des méthodes de destruction des médias ;

2. *Sécurité* – La différence entre la suppression et l'effacement est souvent mal comprise et parfois confondue. Il est important pour les entreprises de comprendre que si les données sont supprimées, elles sont récupérables, mais si elles sont effacées de façon sécurisée, elles sont irrécupérables ;
3. *Évoluer avec son temps* – L'accent mis sur l'effacement des données n'est pas nouveau, comme le déchiqueteur de papier était un appareil de bureau incontournable dans les années 1980, un processus d'effacement complet est impératif aujourd'hui ;
4. *Être une entreprise responsable vis-à-vis de l'écologie* – La plupart des équipements électriques peuvent être recyclés : des serveurs et des ordinateurs de bureau aux ordinateurs portables et aux smartphones.

E. Obligation d'informer les sous-traitants

Dans le cas où le responsable du traitement a déjà rendu publiques les données à caractère personnel et qu'il est tenu de les effacer, il devra, compte tenu des technologies disponibles et des coûts de mise en œuvre, prendre des mesures raisonnables, y compris d'ordre technique, pour informer les tiers responsables du traitement qui traitent également ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.

F. Le droit n'est pas absolu (partie 2)

La personne concernée ne pourra pas exiger l'effacement de ses données à caractère personnel dans la mesure où ce traitement est nécessaire :

1. à l'exercice du droit à la liberté d'expression et d'information ;
2. pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union européenne ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

3. pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9.2.h et 9.2.i, ainsi qu'à l'article 9.3 du RGPD ;
4. à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89.1 du RGPD, dans la mesure où le droit à l'effacement est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ou
5. à la constatation, à l'exercice ou à la défense de droits en justice.

Le droit à l'oubli (appelé aussi alors droit au déréférencement) est apparu suite à la décision dite « *Google Spain* » de la Cour de justice de l'Union européenne du 13 mai 2014 (aff. C-131/12).

Dans cette décision d'importance, la Cour se base sur l'article 12.b de la Directive et sur son article 14.a pour décider que « l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite » (§ 88 de l'arrêt *Google Spain*).

La formulation choisie par le législateur européen pour incorporer cette décision au corpus du RGPD est à regretter.

En effet, alors que le texte de la Directive de 1995 (article 12.b) était général et permettait d'englober tous les traitements qui n'étaient pas conformes à la Directive, celui du RGPD est très précis (voyez les six cas énumérés au point B ci-dessus). Il a perdu la flexibilité de l'article 12.b. de la Directive de 1995.

De plus, le responsable du traitement n'a pas une obligation de résultat vis-à-vis de la personne concernée qui a demandé l'effacement de ses données quant à des données publiques que des tiers traiteraient aussi (point E) et, sans compter que des dérogations existent quant à l'application de ce droit (point F).

La consécration de la jurisprudence Google Spain est donc loin d'être une réussite et reste très technique.

G. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 16 : Les modalités d'exercice des droits des personnes concernées*
- *Fiche de guidance n° 20 : Droit 3 : Le droit de rectification de la personne concernée*

Fiche de guidance n° 22
Droit 5 : Le droit à la limitation du traitement

Article 18 du RGPD

Considérants 67 & 156 du RGPD

A. Un droit aux contours assez flous

Selon l'article 4.3 du RGPD, la « limitation du traitement » est le marquage des données à caractère personnel conservées par l'entreprise concernée en vue de limiter/suspendre leur traitement futur par ladite entreprise. Il s'agit, à la demande de la personne concernée, non pas d'effacer les données personnelles mais de ne plus, temporairement, les soumettre à un quelconque traitement.

Les données ne sont pas effacées. Elles continuent à exister dans les banques de données du responsable du traitement mais elles ne sont plus soumises, pendant un certain délai, à des traitements par le responsable (même si, on peut le concevoir, le fait même de les garder dans les banques de données est aussi un traitement).

Les méthodes visant à limiter le traitement de données à caractère personnel pourraient consister, entre autres, à déplacer temporairement les données sélectionnées vers un autre système de traitement ou une autre banque de données, à rendre les données à caractère personnel sélectionnées inaccessibles aux utilisateurs/employés de la société ou à retirer temporairement les données publiées d'un site internet. Dans les fichiers automatisés, la limitation du traitement devrait en principe être assurée par des moyens techniques de façon que les données à caractère personnel ne fassent pas l'objet d'opérations de traitements ultérieures et ne puissent pas être modifiées. Le fait que le traitement des données à caractère personnel est limité devrait être indiqué de manière claire dans le fichier.

La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique :

1. l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ;
2. le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;
3. le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
4. la personne concernée s'est opposée au traitement en vertu de l'article 21.1 du RGPD, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

   Rappelons que l'article 21.1 permet à la personne concernée de s'opposer, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé :

   – sur l'article 6.1.e du RGPD (« traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ») ou
   – sur l'article 6.1.f du RGPD (« traitement nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant »),
   – y compris un profilage fondé sur ces dispositions.

   Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

B. Une utilisation limitée des données

Lorsque le traitement a été limité, les données à caractère personnel concernées peuvent être traitées sous certaines conditions/circonstances :

1. uniquement dans un objectif de leur conservation ;
2. uniquement avec le consentement de la personne concernée ;
3. pour la constatation, l'exercice ou la défense de droits en justice ;

4. pour la protection des droits d'une autre personne physique ou morale ;
5. pour des motifs importants d'intérêt public de l'Union européenne ou d'un État membre.

Le responsable du traitement devra informer la personne concernée qui a obtenu la limitation du traitement avant que la limitation du traitement ne soit levée.

Il reste dorénavant à voir comment les personnes concernées vont appliquer ce nouveau droit consacré par le RGPD et si ce droit ne sera pas cantonné à des hypothèses très limitées voire marginales.

C. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

➡ *Fiche de guidance n° 16 : Les modalités d'exercice des droits des personnes concernées*

Fiche de guidance n° 23
Droit 6 : Le droit à la portabilité des données

Article 20 du RGPD

Considérants 68 & 156 du RGPD

A. Introduction

Le droit à la portabilité est une nouveauté du RGPD par rapport à la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

En consacrant cette possibilité de recevoir et de (faire) transmettre ses données à caractère personnel à un autre responsable de traitement, le RGPD entend donner plus de contrôle aux personnes concernées par rapport à l'utilisation de leurs données.

Cette possibilité a aussi pour but d'améliorer la circulation des données dans l'UE (le « *free flow of data* ») et d'augmenter la concurrence entre les responsables de traitements, les consommateurs se dirigeant (on l'espère !) vers les prestataires les plus engagés en matière de protection des données personnelles

La portabilité va augmenter la possibilité pour les personnes concernées de changer de fournisseur (briser ce que l'on appelle le « *lock-in* »). Ces derniers vont dès lors devoir augmenter la qualité de leurs services (et en créer de nouveaux) pour maintenir les clients et leurs données chez eux.

B. Un droit double

Dès le moment où les données sont collectées, le responsable du traitement doit informer la personne concernée de l'existence de ce nouveau droit.

Il doit le distinguer des autres droits, notamment en précisant les données susceptibles de faire l'objet d'une portabilité.

Le Groupe de Travail « Article 29 » recommande en outre de signaler aux personnes concernées l'existence de ce droit, en cas de fermeture de leurs comptes, afin de faciliter le stockage et le transfert des données par la personne concernée avant qu'elle ne mette fin au contrat la liant au responsable du traitement.

L'exercice par la personne de son droit à la portabilité ne devra pas la priver de l'exercice des autres droits qui lui sont reconnus par le Règlement européen. Ainsi, le droit à la portabilité ne devra, par exemple, pas faire obstacle au droit à la suppression des données.

1. Première possibilité : celui de recevoir et de transmettre

Grâce à ce droit, les personnes concernées ont le droit de recevoir dans un format structuré, couramment utilisé et lisible par machine, les données à caractère personnel les concernant et qu'elles ont fournies à un responsable du traitement. Les données devront donc être transmises sous un format interopérable.

Les personnes concernées ont le droit, par après, de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées auparavant y fasse obstacle.

Le Groupe de Travail « Article 29 » insiste, dans ses lignes de conduite, sur le fait que le nouveau responsable de traitement devra se conformer à son tour au Règlement européen, et respecter, entre autres, les principes de l'article 5 du RGPD.

Conditions

1. Le droit doit être exercé par la personne concernée (ou son mandataire).
2. Il permet de recevoir les données personnelles.
3. Et de les transmettre à un autre responsable de traitement.
4. Sans que le responsable de traitement qui doit les envoyer puisse s'y opposer.
5. Le droit concerne uniquement les données que la personne concernée a fournies au responsable.
6. La transmission doit se réaliser dans un format structuré, couramment utilisé et lisible par machine (ceci afin de favoriser l'interopérabilité des systèmes).

7. L'exercice du droit ne peut porter pas atteinte aux droits et libertés de tiers.

   La transmission ne peut empêcher les tiers d'exercer les droits qu'ils ont du RGPD. Par exemple, une personne transmet son fichier de contacts à un nouveau service de webmail. Ce nouveau fournisseur de webmail ne peut, directement, envoyer du marketing direct aux contacts contenus dans le fichier d'adresses reçu.

La personne concernée recevra ses données personnelles de la part de son responsable de traitement pour les enregistrer chez elle (sur son PC personnel ou même dans le cloud) pour l'un ou l'autre usage futur. La personne concernée pourra dès lors mieux gérer ses données et pourquoi pas les (faire) réutiliser par après.

Les données à caractère personnel doivent concerner la personne concernée : seules les données à caractère personnel de la personne qui exerce ce droit pourront être « transmises ». Les données anonymes ou celles qui ne concernent pas la personne concernée ne sont pas couvertes par ce droit mais bien, par contre, les données pseudonymisées pouvant clairement être liées à la personne concernée.

Cette possibilité offerte à la personne concernée complémente adéquatement son droit d'accès.

Après avoir exercé son droit à la portabilité de ses données, une personne concernée peut parfaitement continuer à bénéficier des services du responsable de traitement concerné. En effet, l'exercice de ce droit n'est pas directement lié à celui demandant l'effacement de ces données.

Une personne concernée pourrait parfaitement exercer son droit d'accès afin de connaître l'étendue de ses droits collectées par un responsable de traitement et, par après, exercer son droit à la portabilité sur la base de l'information qu'elle a reçue. Ou exercer son droit à la portabilité et vérifier si tout a été bien transmis en exerçant son droit d'accès.

2. Deuxième possibilité : d'un responsable à un autre

De plus, les personnes concernées ont le droit d'exiger que le responsable du traitement transmette directement les données à un autre responsable de traitement « lorsque cela est techniquement possible » ajoute le RGPD.

La transmission peut concerner des fournisseurs qui ne sont pas forcément dans le même secteur d'activités.

3. Conséquences techniques

Le droit à la portabilité des données aura des implications d'un point de vue technique.

Le RGPD n'oblige pas les responsables à développer des formats de traitement compatibles mais les encourage toutefois à développer des formats interopérables permettant l'exercice du droit à la portabilité (considérant 68 du RGPD). Ce que le RGPD interdit aux responsables, c'est de créer des barrières à la transmission.

Les opérateurs devront donc trouver des solutions techniques afin que la restitution des données aux utilisateurs se fasse dans un format ouvert et standard. De cette manière, les données pourront être lues par tout type de matériel, de manière complète, sans que leur intégrité soit compromise. La question du coût supporté par les entreprises se posera dès lors.

Il reste à voir ce que cela signifiera dans le futur et si les différents responsables de traitement arriveront à s'aligner à moindre coût.

Techniquement, le Groupe de Travail « Article 29 » propose deux moyens pour la mise en œuvre du droit à la portabilité des données :

1. la mise à disposition de l'utilisateur d'un fichier contenant l'ensemble des données portables ;
2. la fourniture d'outils automatisés et sécurisés (comme des API pour « *Application Programming Interface* » ou interface de programmation applicative qui permet à deux logiciels de communiquer entre eux) pour l'export de données.

   Ces API devraient permettre aux personnes concernées de réaliser leur requête directement depuis leur ordinateur ou depuis l'application d'une tierce partie ou même de permettre à un tiers de l'exercer en leur nom. Cette possibilité devrait aussi permettre aux personnes concernées de mieux gérer leurs demandes successives (ne pas avoir à tout retélécharger et n'avoir à télécharger que ce qui a été ajouté depuis le dernier téléchargement).

Le Groupe de Travail précise aussi que le responsable du traitement peut, s'il le souhaite, faire appel à un système de gestion des informations personnelles dédié (ou « *Personal Information Management System* », PIMS) pour permettre aux personnes concernées de récupérer leurs données, les conserver et accorder à des entreprises tierces l'autorisation d'y accéder, de manière à faciliter leur transfert à une autre.

L'utilisation d'un tel outil permet d'éviter deux écueils :

1. premièrement, un PIMS va s'assurer que l'individu puisse récupérer ses données dans un format structuré et interopérable, de manière à ce que celui-ci puisse analyser ses données et les transmettre très simplement à qui il le souhaite ;

2. deuxièmement, un PIMS est un moyen pour les entreprises de mettre à disposition les données de leurs utilisateurs et de récupérer des données qui proviennent de divers acteurs par le biais d'un interlocuteur unique, sans avoir à développer et à se brancher à d'innombrables API.

   Les entreprises n'ont donc pas à s'entendre avec chacun des acteurs pouvant être intéressés par les données personnelles qu'elles ont collectées pour créer et maintenir autant de « connecteurs » vers ces sites et vice-versa.

Une fois que les données ont été transmises au nouveau responsable de traitement, elles peuvent être considérées comme ayant été « fournies » par la personne concernée au sens du RGPD.

C. Limites à la portabilité

1. Principe

La personne concernée ne pourra exercer l'une ou l'autre des deux possibilités que si le traitement réalisé grâce aux données (conditions cumulatives) :

1. a été fondé sur
   a) le *consentement* (art. 6.1.a ou art. 9.2.a du RGPD) ou
   b) sur un *contrat* (art. 6.1.b) et
2. a été effectué à l'aide de procédés automatisés (cela ne couvre donc pas les dossiers papiers).

L'exercice du droit à la portabilité des données :

1. s'entend sans préjudice de l'article 17 du RGPD (« Droit à l'effacement ») ;
2. ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
3. on l'a dit, ne porte pas atteinte aux droits et libertés de tiers.

2. Précisions

La compréhension du champ d'application du droit à la portabilité n'est pas si évidente.

Tentons d'y voir plus clair.

Seront compris dans le champ d'application de ce nouveau droit :

1. les données personnelles fournies directement par la personne concernée au responsable du traitement lorsqu'elle a complété, par exemple, en ligne un questionnaire ou un formulaire ;

2. les données que la personne concernée a fournies indirectement au responsable du traitement découlant de son activité, telles que la liste des musiques qu'elle a écoutées ou encore la liste des vêtements qu'elle a pu consulter sur un site d'achat ;
3. les données qui ont été générées par les activités de la personne concernée auprès du responsable de traitement. Par exemple, les données générées par l'utilisation d'un terminal ou d'un service du responsable du traitement par la personne (historique de recherche, historique d'achats, données de trafic, données de localisation, etc.) sont donc visées.

Ne seront pas compris dans le champ d'application du droit :

1. les données qui ont été créées sur la base de l'observation des activités de la personne concernée.

   La portabilité ne concernera pas les données qui sont créées par le responsable du traitement (un profil de clients par exemple) sur la base des données transmises par la personne concernée (« *inferred data and derived data* » en anglais). En effet, ces données « secondaires » car générées par un traitement initial de données sont des informations qui font souvent véritablement partie du savoir-faire des sociétés qui traitent ces données. Il est donc logique qu'elles soient exclues du champ d'application du droit à la portabilité du RGPD.
2. les données traitées sur la base d'une obligation légale ne sont pas concernées (données sociales collectées par l'employeur par exemple) ;
3. les données qui peuvent porter atteinte aux droits des tiers (voyez *infra*).

À l'inverse, la portabilité ne concerne pas uniquement les données qui sont nécessaires au fait de changer de fournisseur. Ce sont toutes les données qui peuvent être concernées.

Imaginons un consommateur qui remplit en ligne un formulaire sur un site de recherche d'emploi. Sur demande du consommateur, l'éditeur du site sera tenu de restituer ou transférer les données transmises par lui (nom, prénom, expériences professionnelles, diplômes …) ou collectées du fait de son activité (types de recherche sur le site, annonces consultées …). En revanche l'éventuel profil établi par le site à la suite d'entretiens ou du fait du résultat de recoupement de fichiers ou d'analyses des annonces consultés, refusés … reste la propriété de l'éditeur qui n'aura pas à le transférer.

D. Données de la personne concernée qui contiennent des données de tiers

Le droit à la portabilité des données ne doit pas porter atteinte aux droits et libertés d'autres personnes. De plus, le « nouveau » responsable de traitement

ne doit, par exemple, pas traiter les données pour une autre finalité que celle initialement prévue pour ne pas porter atteinte aux droits et libertés des tiers. Ces derniers incluent notamment le secret des affaires et la propriété intellectuelle selon le Groupe de Travail « Article 29 ».

Les données doivent concerner la personne qui en demande la portabilité. Cette exigence soulève la question du transfert de données lorsque celles-ci comprennent des données relatives à des tiers. C'est par exemple le cas lorsque l'utilisateur d'un service de messagerie demande la portabilité de ses conversations avec ses contacts. Dans un tel cas, bien que la demande porte sur des données concernant également des tiers, le responsable du traitement doit y répondre.

Si ces données sont par la suite transmises à un autre responsable du traitement, celui-ci ne pourra les traiter d'une manière susceptible de porter atteinte aux droits et libertés de ces personnes tierces.

Cela pourrait être le cas si celles-ci ne sont pas informées et ne peuvent pas exercer leurs droits (droit de rectification, etc.). Le traitement qui sera effectué par le nouveau responsable du traitement devra avoir un fondement autre que le consentement de la personne concernée ou l'existence d'un contrat auquel elle est partie prenante.

L'article 6 du RGPD énonce les fondements possibles d'un traitement (consentement, existence d'un contrat, intérêts légitimes, etc.). Le traitement devra donc être fondé sur l'un des autres cas possibles, tel que les intérêts légitimes poursuivis par le responsable du traitement.

En reprenant l'exemple du service de messagerie, il n'y aura donc pas atteinte aux droits et libertés des tiers si les données sont utilisées par le nouveau responsable du traitement pour la même finalité. En revanche, il y aura atteinte si les données sont par exemple utilisées à des fins de marketing.

Afin de limiter les risques d'atteinte aux droits et libertés des tiers, les responsables du traitement pourraient alors mettre en place des outils permettant aux personnes concernées de sélectionner uniquement les données pertinentes et d'exclure les données de tiers, ou encore des outils permettant de recueillir le consentement des tiers.

E. Les Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail « Article 29 » a adopté, le 5 avril 2017, des Lignes directrices en rapport avec le droit à la portabilité des données (disponibles dans toutes les langues de l'UE sur le site internet du Groupe de Travail) (« Lignes directrices relatives au droit à la portabilité des données », Réf. WP 242 rev.01).

Retenons encore ces quelques précisions fortes utiles et issues de ces Lignes directrices.

Les responsables de traitement qui réalisent la portabilité demandée par une personne concernée ne sont pas responsables par après des actes accomplis par lesdites personnes concernées ou par les responsables de traitement qui ont reçu les données. Ils ne sont pas responsables de la conformité au RGPD du responsable de traitement qui a reçu les données.

Un responsable de traitement ne peut retenir les données au-delà de la période de rétention juste pour peut-être pouvoir satisfaire l'exercice du droit à la portabilité.

Un responsable de traitement doit mettre en place des mesures techniques afin que son ou ses sous-traitants puissent l'aider à satisfaire à ce droit à la portabilité.

Dans le cas de responsables conjoints, le contrat entre eux devrait clairement spécifier les obligations de chacun des responsables en cas d'exercice de ce droit à la portabilité.

Le responsable du traitement qui reçoit les données doit s'assurer que ce qu'il reçoit et va traiter est nécessaire et suffisant par rapport aux nouveaux traitements envisagés.

En réalité, le responsable du traitement qui reçoit les données devient en quelque sorte un nouveau responsable de traitement par rapport aux données transmises. Il doit dès lors aussi satisfaire à tous les principes de l'article 5 du RGPD.

Notons qu'un responsable de traitement est obligé de satisfaire à la demande de transmettre les données de ses personnes concernées mais qu'il n'est pas obligé de recevoir des données transmises par une personne concernée. La réception n'est qu'une faculté pas une obligation. De même, le responsable qui reçoit n'est pas obligée d'avoir déjà un système qui supporte le format des données transmises.

Il serait aussi bien que le responsable de traitement (ré-)informe les personnes concernées de l'existence de ce droit lorsque les personnes concernées entendent clôturer leur relation avec le responsable en question.

Parallèlement, il serait bien que les responsables préviennent les personnes concernées des données qui sont strictement nécessaires pour leurs activités afin d'empêcher que les personnes concernées ne demandent à transmettre des données non utiles.

Dans le cas où le secteur concerné n'a pas mis en place des formats communs, il est conseillé aux responsables de traitement de fournir les données en utilisant des formats libres communément utilisés (p.ex. XML, JSON, CSV…) accompagnées des métadonnées nécessaires. Les PDF sont à déconseiller puisqu'ils ne permettent pas la réutilisation des données qui y sont reprises.

Les responsables de traitement doivent fournir, selon l'art. 12.1 du RGPD, un aperçu des données transmises « d'une façon concise, transparente,

compréhensible et aisément accessible, en des termes clairs et simples » d'une telle manière que la personne concernée comprenne quelles sont les informations qu'elle a reçues et quelles sont les informations qu'elle doit transmettre à un autre responsable de traitement en fonction de la finalité voulue.

Ne pas oublier non plus que les responsables de traitement doivent toujours traiter les données « de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) » (art. 5.1.f du RGPD).

Ils devront s'assurer que les transmissions soient réalisées de la manière la plus sécurisées possibles par l'utilisation par exemple de la cryptographie.

Les mesures utilisées ne doivent pas être excessives et surtout ne pas empêcher l'exercice du droit à la portabilité (ne pas être payantes).

Toutefois, c'est à la personne concernée d'être sûr qu'elle stocke les données reçues dans un environnement suffisamment sécurisé.

F. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

➡ *Fiche de guidance n° 16 : Les modalités d'exercice des droits des personnes concernées*

Fiche de guidance n° 24
Droit 7 : Le droit d'opposition à un traitement

Article 21 du RGPD

Considérants 65, 70 & 73 du RGPD

A. Introduction

Dans certains cas de figure, une personne concernée a le droit de s'opposer à tout moment et pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant.

Ce droit existait déjà à l'article 14 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Le RGPD le précise et l'étend.

B. Limites

Une personne concernée ne peut s'opposer à tout traitement. Certaines limites ont été posées à ce droit.

En effet, elle ne pourra exercer son droit d'opposition que si le traitement est fondé sur :

1. l'article 6.1.e (« traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement »), y compris à un profilage fondé sur cet article 6.1.e ou

2. l'article 6.1.f (« traitement nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant »), y compris à un profilage fondé sur cet article 6.1f.

Dans le cadre de l'utilisation de services de la société de l'information (internet), la personne concernée peut exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.

Lorsque ses données à caractère personnel sont traitées à des fins de prospection (marketing direct), la personne concernée a le droit de s'opposer à tout moment et sans justification aucune au traitement de ses données à de telles fins de prospection, y compris au profilage dans la mesure où le profilage est lié à une telle prospection.

C. Conséquences pour le responsable du traitement

Si la personne concernée a exercé son droit d'opposition, le responsable du traitement ne pourra plus traiter ses données à caractère personnel.

Il pourra néanmoins continuer à traiter les données à caractère personnel concernées s'il démontre qu'il existe des motifs légitimes et impérieux pour :

1. le traitement en question et qui prévalent sur les intérêts et les droits et libertés de la personne concernée ou
2. la constatation, l'exercice ou la défense de droits en justice.

Lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données à caractère personnel ne sont plus traitées à ces fins. Ici, le responsable devra donc s'exécuter sans pouvoir s'y opposer aucunement.

Le responsable du traitement a l'obligation, au plus tard au moment de la première communication avec la personne concernée, de lui faire connaître clairement et séparément de toute autre information l'existence de ce droit d'opposition.

D. Différences avec la Directive de 1995

La Directive de 1995 reprenait déjà ce droit d'opposition en son article 14 :

« Article 14

Droit d'opposition de la personne concernée

Les États membres reconnaissent à la personne concernée le droit :

a) au moins dans les cas visés à l'article 7 points e) et f), de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation

particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire du droit national. En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données ;

b) de s'opposer, sur demande et gratuitement, au traitement des données à caractère personnel la concernant envisagé par le responsable du traitement à des fins de prospection

ou

d'être informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Les États membres prennent les mesures nécessaires pour garantir que les personnes concernées ont connaissance de l'existence du droit visé au point b) premier alinéa. »

Il y a de subtiles différences entre la version de 1995 et celle du RGPD :

1. les mots « au moins dans les cas visés à l'article 7 point e) et f) » de la Directive n'ont pas d'équivalent dans le RGPD.

   L'expression « au moins » traduit le fait que les points .e et .f de l'article 7 ne sont que des exemples d'application du droit d'opposition. Le RGPD précise lui que le droit d'opposition ne peut s'exercer que vis-à-vis d'un traitement « fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions ».

   Le droit d'opposition est donc dorénavant limité aux traitements fondés sur l'article 6.1.e et f. Il n'est donc plus général. Il y a donc un recul par rapport à la Directive de 1995 ;

2. la personne concernée doit toujours justifier l'exercice de son droit d'opposition. Le législateur européen a voulu éviter les abus. La Directive de 1995 demandait que la personne concernée n'exerce son droit que si elle a « des raisons prépondérantes et légitimes tenant à sa situation particulière ». Le RGPD est plus simple. Il précise juste que la personne concernée puisse exercer son droit « pour des raisons tenant à sa situation particulière ». L'exigence est donc moins élevée ;

3. le responsable du traitement ne pouvait refuser d'appliquer la demande de la personne concernée, sous la Directive de 1995, que si une disposition issue de son droit national le lui permettait.

   Le RGPD donne la possibilité au responsable du traitement de démontrer l'existence de motifs légitimes et impérieux de nature à prévaloir sur le droit d'opposition. La différence est d'importance et risque de réduire significativement ce droit d'opposition.

E. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 16 : Les modalités d'exercice des droits des personnes concernées*
- *Fiche de guidance n° 25 : Droit 8 : Le droit à ne pas faire l'objet d'une décision automatique, y compris le profilage*
- *Fiche de guidance n° 44 : le RGPD et le (direct) marketing*

Fiche de guidance n° 25

Droit 8 : Le droit à ne pas faire l'objet d'une décision automatique, y compris le profilage

Article 22 du RGPD

Considérants 60, 71 & 72 du RGPD

A. Décision individuelle automatisée, y compris le profilage

1. Règle générale

Comme la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données avant lui, le RGPD comporte une interdiction générale pour une entreprise de prendre une décision concernant un individu d'une manière totalement automatisée, y compris le profilage.

L'article 22 du RGPD précise en effet que la personne concernée a « le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. ».

Le RGPD prévoit toutefois un certain nombre d'exceptions.

Exemple de décision automatisée :

- le rejet automatique d'une demande de crédit en ligne
- évaluation d'un risque de crédit
- détermination d'une prime d'assurance
- recrutement en ligne avec ou sans intervention humaine

Définition et techniques mises en œuvre

Toute personne a le droit d'être informée de l'existence d'un profilage et des conséquences de celui-ci.

Si l'introduction du concept de « profilage » dans le RGDP est relativement nouvelle, ce n'est en revanche pas le cas pour les décisions individuelles automatisées, qui étaient déjà interdites sous la Directive de 1995.

En effet, le texte de la Directive précisait que les décisions automatiques par principe interdites pouvaient être « destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc. ». Le RGPD ne contient plus dans sa partie normative de précision sur la finalité du profilage.

Définition du profilage

Le profilage est un traitement automatisée de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements (article 4.4 du RGPD). La définition du RGPD est donc très étendue car elle concerne le profilage au sens large plus qu'uniquement des décisions prises de manière automatique (« analyser et prédire des aspects »).

Le « profilage » en tant que technique de traitement automatisé de données à caractère personnel (provenant souvent de sources très diverses) consiste à appliquer, sur la base de corrélations, un « profil » à une personne physique, notamment afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnels (prédiction). Cette analyse se réalise par comparaison de la personne avec d'autres qui lui sont statistiquement similaires. Par exemple, en matière de publicités en ligne, le profilage va permettre, grâce au *tracking* des internautes dans le temps et sur différents sites, de créer des profils très précis de leurs goûts, de leurs caractéristiques, comme l'âge et le sexe et d'afficher en ligne et directement des publicités qui reflètent au mieux leurs intérêts. C'est ce que l'on appelle la publicité ciblée.

Le profilage comprend donc trois étapes :

1. la collecte à grande échelle de données personnelles concernant le comportement d'individus ;
2. une analyse très fine grâce à de puissants algorithmes de ces données afin d'établir des corrélations, des liens entre certaines données et certains comportements aboutissant à la création de profils ou de segments ;
3. l'application de ce profil/segment à un individu.

   Il s'agit ici d'appliquer le profil de groupe à une personne à partir des données personnelles recueillies de cette personne identifiée ou identifiable afin de lui attribuer des données nouvelles qui sont celles de la catégorie à laquelle elle appartient.

Chacune de ces trois étapes représente en réalité une activité de traitement qui tombe dans le champ d'application de la définition du profilage au sens du RGPD.

Le but du profilage est de « placer », « catégoriser », « segmenter » au mieux les individus. Il s'agit de définir un ensemble de données qui caractérise une catégorie d'individus pour les appliquer à un individu dans le but de réaliser des prédictions ou des analyses à propos, par exemple, de leur capacité à effectuer une tâche, de leurs intérêts ou de leur comportement probable.

Les sociétés collectent elles-mêmes ou acquièrent de sociétés tierces des données à caractère personnel voire demandent à des sociétés d'enrichir ou d'améliorer/corriger les données qu'elles possèdent sur leur clientèle. Les sociétés par après croisent ces fragments d'informations collectées ou récupérées afin de reconstituer le profil le plus précis possible de leurs clients/prospects. En effet, au plus le profil est complet, au plus il a de la valeur pour la société qui pourra le connecter avec des offres de plus en plus personnalisées. Les offres deviennent dès lors de plus en plus précises et donc possibles d'être acquises par ces clients « profilés » au plus près. C'est pour cette raison que les internautes sont de plus en plus suivis de site web en site web.

La technique du profilage peut avoir des incidences pour les personnes concernées car ils sont placés automatiquement dans des catégories prédéterminées, très souvent à leur insu. Les profils, lorsqu'ils sont attribués à une personne concernée, permettent de générer des nouvelles données à caractère personnel qui ne sont pas celles que la personne concernée a communiquées au responsable de traitement ou dont elle peut raisonnablement présumer la connaissance par le responsable de traitement.

Le danger d'un profilage mal réalisé est d'augmenter les différences préexistantes. Tout profilage devrait être guidé par des lignes directrices claires qui devraient être rendues publiques dans le cas où le profilage a eu des conséquences négatives pour un individu.

Afin d'assurer un traitement équitable et transparent à l'égard de la personne concernée, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées, le responsable du traitement devrait utiliser des procédures mathématiques ou statistiques adéquates et correctes pour son profilage.

Le responsable du traitement devrait aussi appliquer des mesures techniques et organisationnelles appropriées pour faire en sorte, en particulier, que les facteurs qui entraînent des erreurs dans les traitements de ses données à caractère personnel soient corrigés et que les risques d'erreur soient donc réduits au minimum.

Enfin, le responsable devrait aussi sécuriser les données à caractère personnel d'une manière :

- qui tienne compte des risques susceptibles de peser sur les intérêts et les droits de la personne concernée et

- qui prévienne, entre autres, les effets de discriminations à l'égard des personnes physiques fondées sur l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, ou l'orientation sexuelle.

2. Champ d'application de l'article 22 du RGPD

L'article 22 du RGPD vise le profilage et les décisions fondées exclusivement sur un traitement automatisé.

Les décisions fondées exclusivement sur un traitement automatisé sont prises sans aucune intervention humaine et sur la base de données directement fournies par la personne concernée ou déduites du profil que le responsable du traitement a créé de la personne.

La prise de décision et le profilage automatisés fondés sur les catégories particulières de données à caractère personnel de l'article 9 du RGPD ne sont autorisés que dans des conditions spécifiques.

L'internet des objets (« IoT ») permet de tracer les personnes de plus en plus facilement et jusque dans leurs moindres faits et gestes. Ces objets connectés créent des milliards d'informations, de données informatiques (big data). Pour stocker et gérer/traiter ces données massives, les sociétés ont de plus en plus besoin du *cloud computing*. Les entreprises vont utiliser des techniques de forage de données (« *data mining* ») afin de dresser des profils très précis des individus pour arriver à prédire ce que le consommateur veut ou va acheter (intelligence artificielle).

Le Groupe de Travail « Article 29 » considère que le profilage intervient dans trois possibilités :

i. le profilage de manière générale ;

ii. les décisions automatisées fondées sur du profilage (ex. : un employé d'une entreprise doit décider si un individu se voit octroyer un prêt. L'employé va fonder sa décision sur un profil produit de manière automatique) et

iii. les décisions exclusivement automatiques incluant le profilage (Article 22 du RGPD) (ex. : un algorithme informatique décide lui seul de la décision de l'octroi ou non du prêt et ce sans aucune intervention humaine).

3. Droit d'opposition partiel contre le profilage

La personne concernée a le droit de s'opposer à tout moment et pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6.1.e (« traitements nécessaires

à l'exécution d'une mission d'intérêt public ») ou 6.1.f (traitements nécessaires aux fins des intérêts légitimes » du responsable du traitement), y compris un profilage fondé sur ces dispositions (article 21.1 du RGPD).

Nous l'avons lu, il sera demandé à la personne concernée de dire pourquoi (« tenant à sa situation particulière ») elle veut s'opposer à l'utilisation de ses données pour la création de profils. Gageons que, dans pas longtemps, les associations de défense des consommateurs vont standardiser ce genre d'argumentation afin de faciliter la vie de ceux qui veulent s'opposer à l'utilisation de leurs données à des fins de profilage.

Dans le cas où la personne concernée argumente et exerce son droit d'opposition pour un tel traitement et si le traitement était fondé sur l'une des deux bases juridiques mentionnées, le responsable du traitement ne pourra plus traiter les données à caractère personnel *sauf* s'il arrive à démontrer qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée ou si le traitement est nécessaire pour la constatation, l'exercice ou la défense de droits en justice.

Dans le cas où les données à caractère personnel sont traitées à des fins de prospection (marketing direct) par le responsable du traitement, la personne concernée a le droit de s'opposer à tout moment (et sans justification aucune) au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection.

Lorsque la personne concernée s'oppose au traitement à des fins de prospection, le responsable du traitement devra arrêter directement un tel traitement.

Au plus tard au moment de la première communication avec la personne concernée, le droit d'opposition partiel au profilage est explicitement, clairement et séparément de toute autre information, porté à l'attention de la personne concernée.

4. Droit à ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé

Rappelant le principe déjà énoncé à l'article 15 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, l'article 22 du RGPD énonce que :

> « Toute personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. ».

Notons que le RGPD ne définit pas ce qu'il faut entendre par « produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ». Il faudra attendre une décision de la Cour de justice de l'Union européenne pour avoir plus de précisions à ce sujet. La Directive de 1995 précisait, elle, que la décision devait produire « des effets juridiques à son égard ou l'affectant de manière significative ».

Le Groupe de Travail « Article 29 » donne dans ses Lignes directrices d'octobre 2017 déjà quelques éclaircissements à ce propos.

Une activité de traitement aura des *effets juridiques* si elle a des conséquences sur des droits d'un individu comme son droit d'association, de vote ou d'intenter une action judiciaire ou ses droits contractuels.

Une opération de traitement affectera une personne concernée *de manière significative de façon similaire* dans le cas où elle l'affecte d'une manière significative et ce en fonction des circonstances, du comportement ou des choix de la personne. La décision pourrait avoir comme conséquence ultime, par exemple, d'exclure ou de discriminer la personne concernée. Le considérant 71 du RGPD cite en exemple d'une telle décision le rejet automatique d'une demande de crédit en ligne.

Le Groupe de Travail « Article 29 » envisage que cette notion puisse s'appliquer à certaines formes de publicité comportementale, notamment lorsqu'elle vise des personnes vulnérables. Le Groupe considère que des décisions automatisées qui résultent dans l'octroi de prix différents pourraient aussi affecter une personne de manière significative si, par exemple, des prix prohibitifs empêchent une personne d'avoir accès à certains biens ou services.

5. Exceptions à l'interdiction générale

La personne ne peut s'opposer à faire « l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire » lorsque la décision en question (ou inversément, le responsable du traitement peut prendre une décision entièrement automatique relative à une personne concernée lorsque la décision) :

1. est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;
2. est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ou
3. est fondée sur le consentement explicite de la personne concernée.

Même si le responsable du traitement peut prendre une décision automatisée à l'égard d'une personne concernée (car il dispose par exemple du

consentement explicite de celle-ci), la décision ne pourra être fondées sur les catégories particulières de données à caractère personnel visées à l'article 9.1 du RGPD. À nouveau, la décision pourra quand même être fondée sur des données particulières dans le cas où la personne concernée a donné son consentement explicite ou si le traitement est nécessaire pour des motifs d'intérêt public et si des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ont été mises en place.

On le voit, les exceptions possibles à l'interdiction de principe de prendre des décisions totalement automatisées sont étendues par rapport au texte de la Directive de 1995.

Ainsi, il peut dorénavant être dérogé à l'interdiction lorsque la décision est fondée sur le consentement explicite de la personne concernée, possibilité inexistante dans la Directive. L'ajout de cette possibilité pourrait vider le principe de l'interdiction de son sens lorsque l'on se rend compte que les internautes donnent aisément leur consentement pour pouvoir utiliser de nombreux services numériques sans avoir conscience de leur mode de fonctionnement.

Notons que le responsable du traitement ne peut échapper à l'interdiction des décisions automatisées juste en intercalant une personne qui va de manière automatique et à chaque fois appliquer la décision proposée par l'ordinateur.

Dans le cas où la personne concernée ne peut s'opposer à faire l'objet d'une décision automatisée, le responsable du traitement devra mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée.

Le responsable du traitement devra au moins permettre à la personne concernée :

1. d'obtenir une intervention humaine de la part du responsable du traitement.

   La personne concernée pourrait demander à obtenir la logique qui sous-tend le profilage afin de comprendre l'algorithme qui a été utilisé dans le traitement de ses données à caractère personnel ;

2. d'exprimer son point de vue et de contester la décision prise automatiquement.

   L'employé de la société que la personne concernée aura au bout du fil doit avoir la possibilité de véritablement déroger à la décision prise par la machine. Idéalement, en cas de contrôle d'une autorité de contrôle, la société devrait pouvoir prouver qu'effectivement, l'intervention humaine a, dans un certain nombre de cas, dérogé effectivement à la décision automatique (même si ce pourcentage est très minime).

6. Obligation d'information du responsable du traitement

L'article 13.2.f (et 14.2.g) du RGPD oblige le responsable du traitement à fournir à la personne concernée au moment où les données à caractère personnel sont obtenues :

> « l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ».

Autrement dit, dans le cas où le responsable entend prendre des décisions automatisées au sens de l'article 22 du RGPD (en ce compris un profilage), il devra :

- prévenir lorsque les données personnelles de la personne concernée sont obtenues que tel sera le cas ;
- lui fournir des informations suffisamment utiles concernant la logique sous-jacente à la prise de décision automatisée ;
- lui expliquer l'importance et les conséquences prévues concernant la prise de décision automatisée en ce qui la concerne.

L'explication aux personnes concernées, accompagnée d'exemples si possible, sur « la logique sous-jacente », « l'importance et les conséquences » des décisions individuelles automatisées doit être simple, compréhensible et utile, sans avoir besoin d'aller dans le détail du fonctionnement de l'algorithme (serait-ce d'ailleurs possible quand on sait que souvent ces algorithmes sont souvent des boites noires ?). L'information doit quand même être suffisante que pour permettre à la personne concernée de comprendre comment la décision automatique a été prise et sur quelles bases. Le responsable du traitement devrait fournir à la personne concernée un moyen facile pour pouvoir exercer ses droits dont celui à une intervention humaine dont nous parlions précédemment.

L'article 13 renvoie uniquement aux paragraphes 1 et 4 de l'article 22 du RGPD.

Est-ce à dire que lorsque la prise de décision automatique se passe dans le contexte d'une des trois exceptions de l'article 22.2 (contrat-loi-consentement explicite), la personne n'a pas à être informée ? Cela semble illogique et surtout contradictoire avec le fait qu'elle puisse dans le cas de l'article 22.2 faire valoir son point de vue et avoir une chance de renverser la décision automatique.

Pour couper court à ces controverses, le Groupe de Travail « Article 29 » rappelle que le considérant 60 du RGPD précise que la fourniture d'informations par le responsable du traitement à propos de ses activités de profilage fait partie des obligations de transparence imposées par l'article 5.1.a. du RGPD. La personne concernée a le droit d'être informée par le responsable à propos du profilage qu'il réalise et qu'il a, dans certaines circonstances, le droit de s'y

opposer qu'importe si une décision individuelle complètement automatisée fondée sur du profilage a lieu ou pas.

7. Workflow d'analyse d'une décision automatisée

1. la personne concernée a le droit de *s'opposer* à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6.1.e ou 6.1.f du RGPD, y compris un *profilage* fondé sur ces dispositions. Le responsable du traitement peut tenter de contre argumenter ;
2. par principe, une personne *peut s'opposer* au fait qu'elle va subir une décision fondée exclusivement sur un traitement automatisé (à mettre dans cette catégorie les décisions qui sont créées par des algorithmes mais que les humains suivent aveuglément dans tous les cas), y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ;
3. le responsable du traitement devra réaliser une *AIPD* dans le cas où il entend réaliser des traitements à des fins de prise de décisions fondées exclusivement ou non exclusivement sur des traitements automatisés. Dépendant du cas d'espèce, le responsable du traitement devra ou ne devra pas réaliser une AIPD pour d'autres activités de profilage ;
4. la personne concernée a toujours le droit à n'importe quel moment de s'opposer sans avoir à se justifier au traitement de ses données à des fins de *prospection* et donc y compris à du profilage réalisé à des fins de prospection ;
5. *exception* :
   - la personne concernée ne pourra *pas s'opposer* à la prise de décision automatisée dans *trois cas de figure* :
     - lorsque le traitement est nécessaire à l'exécution d'un contrat
     - est autorisé par une Loi
     - la personne a explicitement accepté de faire l'objet d'une décision automatisée ;
   - la personne concernée a alors le *droit* :

     (a) d'obtenir une intervention humaine de la part du responsable du traitement afin d'obtenir une explication quant à la décision prise,

     (b) d'exprimer son point de vue et

     (c) de contester la décision
   - dans le cas où le responsable du traitement envisage de réaliser du profilage ou de prendre des décisions automatisées, il doit *informer* la personne concernée au moment où il obtient ses données personnelles :

– de son droit d'opposition (voir point 1) ;
– de l'existence d'une prise de décision automatisée, y compris un profilage, d'informations utiles concernant la « logique sous-jacente » de la décision automatisée et d'informations sur l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Il s'agit d'une application du *principe de transparence*, principe fondamental du RGPD ;

- la personne concernée pourrait obtenir les informations sous-jacentes aux traitements (en ce compris ceux ayant été nécessaires pour réaliser les différents profils ainsi que les catégories de données qui y ont été nécessaires) dans le cadre de son *droit d'accès*.

B. La Recommandation du 23 novembre 2010 du Conseil de l'Europe

Le Conseil de l'Europe a voté une recommandation sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage.

Cette Recommandation date d'avant le RGPD.

Le Groupe de Travail « Article 29 » rappelle que le RGPD s'est inspiré de la définition de profilage de la Recommandation du Conseil de l'Europe tout en s'en éloignant quelque peu. En effet, le Conseil de l'Europe n'a pas repris dans sa définition de profilage, les activités de traitement qui consistent à classer et catégoriser les individus sur la base de leur âge, sexe, activités professionnelles dans le but de créer des segments.

C. Conséquences

Les conséquences des nouvelles règles du RGPD se feront surtout sentir au niveau des départements marketing des sociétés dans une mesure toutefois qu'il reste à analyser de manière plus approfondie (analyse qu'il s'agira surtout de réaliser et de compléter lorsque les nouvelles règles en matière de *ePrivacy* seront définitives).

Tentons toutefois ici de poser les bases de la future discussion.

Quand se termine un profilage et quand commence la sélection ?

Par exemple, un service totalement personnalisé ainsi que les techniques de publicités personnalisées sont habituellement basés sur une sélection

elle-même fondée sur des profils de comportement et d'achat. Faudra-t-il dorénavant disposer d'un consentement explicite pour réaliser ces opérations ? Il semble bien que oui.

Notons que la notion de « *direct marketing* » (« prospection » dans la version française du Règlement) n'a pas été définie dans le RGPD.

Selon les nouvelles règles, il faut distinguer deux sortes de profilage :

1. le profilage qui n'a pas d'effet juridique direct.

   La personne concernée a le droit de s'opposer à tout moment et pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6.1.e du RGPD (traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement) ou 6.1.f (traitement nécessaire aux intérêts légitimes du responsable du traitement), y compris à un profilage. Lorsque la personne concernée s'est opposée avec succès à ce que ses données ne servent plus à réaliser du profilage (la concernant et concernant d'autres personnes ?), le responsable du traitement ne traite plus les données à caractère personnel dans un but de profilage sauf s'il démontre qu'il possède des motifs légitimes et impérieux pour un tel traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

   Un test d'équilibrage est ici à réaliser. Il lui faudra prendre en compte certains facteurs comme la nature et la source de l'intérêt légitime.

   L'analyse portera sur le fait de savoir si le traitement est nécessaire pour l'exercice d'un droit fondamental ou s'il bénéficie à une communauté concernée, quel est l'impact du profilage sur les personnes concernées, quelles étaient leurs attentes raisonnables lors de la collecte de leurs données, etc. Le test devra aussi tenir compte des garanties apportées par le responsable du traitement pour limiter l'impact sur les personnes concernées comme le respect du principe de minimisation de l'utilisation des données personnelles, l'utilisation de technologies de protection de la confidentialité.

   Rappelons que lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection. La personne concernée ici ne doit pas du tout justifier son choix.

2. le profilage qui a un effet juridique sur la personne.

   La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Toutefois, la personne concernée *ne peut s'opposer* à cette décision automatique qui inclut le profilage lorsque cette décision automatique est soit nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, soit autorisée par le droit de l'Union ou le droit de l'État membre du responsable du traitement ou est fondée sur le consentement explicite de la personne concernée.

Le responsable du traitement devra dans ce cas mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

Dès lors, quand la personne concernée ne peut-elle pas s'opposer à un profilage ?

Il se déduit de ce qui précède que :

- dans le cas d'un profilage qui n'a pas d'effet juridique sur elle, la personne concernée ne pourra pas s'y opposer lorsque le profilage est lié à un traitement fondé sur une des autres bases juridiques de l'article 6 du RGPD (autre donc que l'exécution d'une mission d'intérêt public ou les intérêts légitimes du responsable du traitement) ;
- dans le cas d'un profilage qui a des effets juridiques sur elle, la personne concernée ne pourra pas s'y opposer si le profilage est nécessaire pour la conclusion ou l'exécution d'un contrat, si le profilage est autorisé par le droit de l'Union ou par son droit national (cas du profilage d'un client réalisé pour respecter la législation financière appelée Mifid ou la réglementation anti-blanchiment par exemple) ou si elle y a consenti. Elle ne pourra pas s'opposer au profilage en soi mais pourra toujours contester la décision auprès d'une personne physique et peut-être obtenir une autre décision.

D. Le profilage doit également respecter l'ensemble des principes du RGPD

Une société qui entend utiliser les données de ses clients ou de ses prospects doit toujours respecter l'ensemble des exigences du RGPD. Toutefois, dans le cadre d'une prise de décision purement automatique ou de profilage, le respect de ces principes pourrait poser quelques difficultés.

Le responsable du traitement doit, par exemple, s'assurer de l'exactitude des données utilisées pour créer les profils ainsi que de la qualité de ses algorithmes. Il doit éviter que la création de ses profils ne comporte des erreurs.

C'est pourquoi, il devra être aussi transparent que possible (mais ne pas aller jusqu'à dévoiler ses secrets d'affaires) sur ses méthodes de profilage.

Le responsable du traitement devra procéder à des évaluations d'impact (AIPD) en cas de profilage ou d'évaluation systématique et approfondie d'aspects personnels de personnes physiques, profilage ou évaluation fondé sur des traitements automatisées. L'AIPD devra être réalisée lorsque de ces évaluations ou de ce profilage des décisions ayant des effets juridiques à l'égard d'une personne physique sont prises (article 35.3.a du RGPD).

Comme en matière de big data, ce sont principalement les principes de finalité et de rétention qui poseront le plus de problème. En effet, il pourrait arriver que le profilage se réalise à l'aide de données collectées auparavant mais pour d'autres finalités.

C'est pourquoi, de manière générale, nous conseillons aux responsables du traitement d'analyser très régulièrement leurs processus de prises de décision automatique et la façon dont les profils sont créés.

E. Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail des autorités de contrôle nationales a adopté le 6 février 2018 des Lignes directrices en la matière. Ces Lignes directrices (nous en avons incorporé certains éléments dans nos explications) sont disponibles pour l'instant uniquement en anglais via le site du Groupe de Travail (« *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation* 2016/679 », Réf. WP 251).

F. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 16 : Les modalités d'exercice des droits des personnes concernées*
- *Fiche de guidance n° 18 : Droit 1 : Le droit d'information des personnes concernées*
- *Fiche de guidance n° 24 : Droit 7 : Le droit d'opposition à un traitement*
- *Fiche de guidance n° 35 : Le big data et le RGPD*

Fiche de guidance n° 26
Les violations de données personnelles

Articles 33 et 34 du RGPD

Considérants 85 à 88 du RGPD

A. Principe

Aujourd'hui, les sociétés créent, produisent et utilisent de plus en plus de données. Et ce de plus en plus vite. Par conséquent, les risques de violations des données à caractère personnel augmentent aussi. Les risques sont non seulement liés à l'augmentation du volume des données mais aussi à la valeur des données concernées (nom, prénom, adresses, anniversaire, données financières, etc.). Aux États-Unis par exemple, un numéro de sécurité sociale se vend, sur le marché noir, en moyenne sept euros, une date de naissance environ deux euros.

Nous créons des données et des informations, sans nous en rendre compte, lorsque nous naviguons sur un site internet, lorsque nous effectuons une recherche en ligne, lorsque nous achetons en ligne, etc.

Au plus les données et leur valeur (ainsi que leur sensibilité) augmentent, au plus, les sociétés sont à risque face aux violations non intentionnelles mais aussi, malheureusement, intentionnelles.

Le RGPD prévoit que les entreprises devront notifier aux autorités de contrôle des données personnelles les violations de données à caractère personnel (fuites de données, accès non autorisé, pertes de données, etc.) sauf si ces violations ne présentent aucun risque. Dans les cas comportant un risque élevé pour les personnes concernées, une notification aussi devra leur être faite de la violation intervenue.

Il convient de constater aussi que la sécurité des données personnelles devra être assurée, en application du Règlement, tant par le responsable de traitement que par le sous-traitant. En effet, l'article 32 du Règlement impose à ces deux acteurs de prendre en compte différents facteurs de sécurité.

Le RGPD prend très au sérieux les failles de sécurité et les violations de données à caractère personnel qui peuvent survenir où que se trouvent les données dans l'entreprise. Les sociétés se doivent dorénavant de correctement savoir quelles sont les données qu'elles possèdent, où se trouvent ces données, de déterminer qui en est responsable (le « *data owner* ») et de bien savoir les contrôler.

Une violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages économiques ou sociaux importants, des dommages physiques, matériels ou même un préjudice moral.

Ces dommages peuvent être de plusieurs sortes :

- une perte de contrôle sur leurs données à caractère personnel ;
- la limitation de leurs droits ;
- une discrimination ;
- un vol ou une usurpation d'identité ;
- une perte financière ;
- un possible renversement non autorisé de la procédure de pseudonymisation ;
- une atteinte à la réputation ;
- une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre ;
- etc.

Les autorités de contrôle des données personnelles devront vérifier si :

1. toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre par le responsable du traitement pour déceler immédiatement si une violation des données à caractère personnel s'est réalisée ou non ;
2. elles, et le cas échéant la personne concernée, ont été informées de la situation rapidement ou dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée.

En pratique

Afin de répondre aux exigences imposées en matière de gestion des failles de sécurité et de pouvoir réagir adéquatement dans le délai très court, il est recommandé aux sociétés de mettre en place dès aujourd'hui les mesures suivantes :

1/ une cellule de crise ;

2/ formaliser une procédure de gestion des violations de sécurité décrivant les grandes étapes de la gestion d'une faille de sécurité, à savoir : identification et correction « technique » de la faille, mesures d'urgence pour remédier aux violations et en atténuer les conséquences négatives potentielles, constitution d'un dossier de preuves techniques et juridiques, dépôt de plainte, déclaration de sinistre auprès de l'assurance, notification à l'autorité de contrôle et communication à la personne concernée le cas échéant, communication « publique » de type « communiqué de presse » éventuellement ;

3/ rédiger des modèles-types : notification à l'autorité de contrôle, communication à la personne concernée, communiqué de presse, etc. ;

4/ élaborer un registre documenté des failles de sécurité, assorti de retours d'expérience constructifs.

Les mesures de sécurité mises en place par le responsable et le sous-traitant doivent avoir pour objectif d'assurer la confidentialité, l'intégrité et la disponibilité du système de traitement des données ainsi que l'accès à celles-ci.

Ces mesures ne peuvent être déterminées qu'après identification des risques. Dès lors, les analyses de risques classiquement utilisées aujourd'hui demeureront un précieux outil.

Le Règlement introduit la notion nouvelle de « résilience constante des systèmes et des services de traitement ».

Selon le glossaire de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) française, la résilience se dit, en informatique, de la « capacité d'un système d'information à résister à une panne ou à une cyberattaque et à revenir à son état initial après l'incident. ».

Les solutions de sauvegarde et le système de redondance devront donc être renforcés.

L'ensemble de ces mesures devront être décrites dans une *politique de sécurité* afin de documenter le respect par le responsable de traitement et le sous-traitant de son obligation d'assurer la sécurité des données personnelles, conformément au principe de responsabilité (*accountability*). En outre, l'exigence d'adaptation des mesures de sécurité imposera d'évaluer régulièrement l'efficacité des mesures prises pour les réajuster le cas échéant.

Les sociétés devront peut-être veiller à la mise en place d'un véritable centre opérationnel de sécurité (SOC) interne ou externe. Le SOC a un rôle de surveillance du système d'information. Ce n'est donc pas à lui qu'incombe la gestion de la crise et il n'a pas vocation à se substituer aux équipes de réponse à incident (CSIRT), même s'il se doit d'être « en interaction forte » avec elles. Le SOC va contextualiser les incidents afin de prévoir la réponse adéquate.

B. Trois hypothèses possibles

Selon le RGPD, en cas de violation de données à caractère personnel, le responsable du traitement devra (trois cas possibles) :

1. notifier l'autorité de contrôle des données personnelles et les personnes concernées si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique ;
2. notifier uniquement l'autorité de contrôle des données personnelles si la violation est susceptible d'engendrer un risque qui n'a pas été catalogué comme élevé pour les droits et libertés des personnes physiques ;
3. ne notifier personne mais juste enregistrer l'incident dans ses registres si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

Le sous-traitant devra notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Détaillons ci-après les deux premiers points, le dernier n'appelant pas plus de commentaire.

1. Risque élevé : notification aux personnes concernées et à l'autorité de contrôle des données personnelles

a. *Délai de la notification*

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement devra communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais afin que celle-ci puisse prendre les précautions qui s'imposent.

Le RGPD ne précise pas expressément s'il convient aussi de notifier l'autorité de contrôle. Toutefois, puisque la société devra le faire si le risque n'a pas été considéré comme élevé pour les droits et libertés des personnes concernées, il semble logique que la société doive aussi réaliser cette notification en cas de risque élevé et dans le fameux délai de 72 heures (pour les modalités, voyez *infra*).

Les entreprises d'assurances sont en discussion avec les autorités de contrôle afin de voir si elles ne pourraient pas recevoir de la part des autorités de contrôle les données agrégées (donc anonymisées) relatives aux notifications en cas de violation. En effet, de telles informations pourraient aider les entreprises d'assurances à mieux comprendre le marché des risques informatiques (du *cyber risk*) et dès lors à mieux établir leurs tarifs en matière de cyber assurances. Ce type d'assurance est train de se développer et ce genre d'informations permettrait d'établir des plans de réponse de la part des compagnies d'assurance plus adéquats et plus rapides en fonction des violations concernées.

b. *Contenu de la notification aux personnes concernées*

La communication à la personne concernée :

1. décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel ;
2. communique le nom et les coordonnées du Délégué à la Protection des Données (DPD) ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
3. décrit les conséquences probables de la violation de données à caractère personnel ;

4. décrit les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Ces communications aux personnes concernées devraient se réaliser en collaboration avec les autorités de protection des données personnelles ou avec les autorités répressives.

En effet, il pourrait arriver qu'il faille adresser rapidement une communication aux personnes concernées afin d'atténuer un risque immédiat de dommage. Dans d'autres situations, il serait au contraire nécessaire de leur communiquer la violation plus tard afin, par exemple, de permettre aux autorités de prendre certaines mesures pour empêcher la poursuite de la violation des données ou pour empêcher la survenance de violations similaires. La communication de certaines violations de données pourrait aussi entraver inutilement des enquêtes sur les circonstances desdites violations.

c. *Pas de notification aux personnes concernées si…*

Toutefois, le responsable du traitement ne devra pas notifier la violation si (trois situations possibles) :

1. première hypothèse (hypothèse où ce sont, par exemple, des données chiffrées qui ont fait l'objet de la violation) (ces notifications n'apporteraient aucune amélioration aux citoyens en matière de respect de la vie privée) :
   a) le responsable avait auparavant pris des mesures de protection techniques et organisationnelles appropriées (en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès comme le chiffrement) et
   b) ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation ;
2. deuxième hypothèse :
   a) il a pris des mesures après la violation et
   b) ces mesures garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser à nouveau ;
3. troisième hypothèse :
   a) la notification exigerait des efforts disproportionnés ;
   b) dans ce cas, le responsable pourra procéder à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de la violation de manière tout aussi efficace.

Dans le cas où le responsable pense pouvoir bénéficier de l'une de ces exceptions, l'autorité de contrôle des données personnelles pourrait réévaluer la situation.

En effet, l'autorité de contrôle peut, après avoir examiné si la violation de données à caractère personnel en question est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède quand même à cette communication.

Nous vous renvoyons au point 2.b pour le contenu de la notification à l'autorité de contrôle qui sera identiquement le même.

2. Le risque est considéré comme non élevé : notification uniquement à l'autorité de contrôle

En cas de violation de données à caractère personnel susceptible d'engendrer un risque qui n'a pas été considéré comme élevé pour les droits et libertés des personnes physiques, le responsable du traitement devra en notifier la violation en question uniquement à l'autorité de contrôle des données personnelles.

a. *Délai de la notification*

La notification doit intervenir, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance (délai très court !). Notons que la notification pourrait être effectuée à partir du site de l'autorité de contrôle au moyen d'un formulaire en ligne. L'autorité belge a mis en place des formulaires électroniques.

Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

Dans le cas où la violation s'est réalisée auprès du sous-traitant, celui-ci devra le notifier au responsable du traitement dans les meilleurs délais après en avoir pris connaissance.

Il convient donc de définir des règles de remontées d'informations dans les contrats conclus avec les sous-traitants par le biais d'une annexe dite PAS (« Plan d'assurance sécurité ») dédiée aux données personnelles afin de s'enquérir auprès de ses prestataires des délais dans lesquels ils sont en capacité de lui notifier toute violation de sécurité.

b. *Contenu de la notification*

La notification devra, à tout le moins :

1. décrire :
   a) la nature de la violation de données à caractère personnel ;

b) les catégories et le nombre approximatif de personnes concernées par la violation ;

c) les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

d) les conséquences probables de la violation de données à caractère personnel ;

e) les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives ;

2. communiquer le nom et les coordonnées du DPD ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

c. *Tenue d'un registre des violations*

Le responsable du traitement documentera dans un registre dédié à cet effet toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permettra à l'autorité de contrôle de vérifier le respect des obligations du responsable de traitement.

C. Lien avec le Règlement notification *ePrivacy* du 24 juin 2013

La Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et services de communications électroniques dans l'Union.

En vertu de l'article 4 de la directive 2002/58/CE, les fournisseurs de services de communications électroniques accessibles au public sont tenus de

notifier les violations de données à caractère personnel aux autorités nationales compétentes et, dans certains cas, aux abonnés et aux particuliers concernés.

Les violations de données à caractère personnel sont définies à l'article 2.i de la directive 2002/58/CE comme des :

> « violations de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans l'Union ».

Un règlement secondaire de 2013 prévoit les règles pratiques d'exécution en matière de notification obligatoire à l'autorité nationale compétente et/ou à l'abonné de violations de données à caractère personnel par les fournisseurs de services de communications électroniques accessibles au public (Règlement (UE) N° 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques).

Les notifications doivent se réaliser via un moyen électronique sécurisé et au plus tard 24h après le constat de la violation, si possible.

Selon le règlement, le constat d'une violation de données à caractère personnel est considéré comme établi dès lors que « le fournisseur dispose d'assez d'éléments indiquant qu'il s'est produit un incident de sécurité ayant compromis des données à caractère personnel pour justifier une notification conformément au présent règlement ».

Les fournisseurs ne doivent pas notifier :

1. les soupçons de violation de données à caractère personnel ;
2. la simple constatation qu'un incident sans disposer d'informations suffisantes, malgré tous les efforts déployés à cette fin par ledit fournisseur.

Comme pour le RGPD, il faut faire une distinction :

1. le fournisseur devra notifier à l'autorité compétente nationale toutes les violations de données à caractère personnel (avec un contenu fixé à l'Annexe I du règlement de 2013) ;
2. le fournisseur devra notifier ET à l'autorité compétente ET à l'abonné/au particulier les violations de données à caractère personnel qui sont susceptibles de porter atteinte aux données à caractère personnel ou à la vie privée (contenu fixé à l'Annexe II du règlement en question).

Afin de savoir si une violation de données à caractère personnel est susceptible de porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'un particulier, il faudra tenir compte des éléments suivants :

1. la nature et la teneur des données concernées, en particulier s'il s'agit de données relatives à des informations financières, de catégories de données particulières visées à l'article 8.1, de la directive 95/46/CE

ainsi que de données de localisation, fichiers journaux internet, historiques de sites web consultés, données relatives au courrier électronique et listes d'appels téléphoniques détaillées ;

2. les conséquences vraisemblables de la violation de données à caractère personnel pour l'abonné ou le particulier concerné, notamment les cas où la violation pourrait entraîner un vol ou une usurpation d'identité, une atteinte à l'intégrité physique, une souffrance psychologique, une humiliation ou une atteinte à la réputation et
3. les circonstances de la violation de données à caractère personnel, en particulier l'endroit où les données ont été volées ou le moment auquel le fournisseur sait que les données sont en possession d'un tiers non autorisé.

La notification à l'abonné ou au particulier devra être effectuée sans retard injustifié après le constat de la violation de données à caractère personnel. Cette notification est indépendante de la notification de la violation de données à caractère personnel à l'autorité nationale compétente. La notification à l'abonné ou au particulier est rédigée dans une langue claire et aisément compréhensible

Comme pour le RGPD, il est prévu des exemptions de notifications à l'abonné/particulier alors que ces notifications auraient dû être réalisées.

En effet, la notification d'une violation de données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si :

1. le fournisseur a prouvé, à la satisfaction de l'autorité nationale compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées (comme des mesures de protection technologiques rendant les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès) et
2. si ces dernières ont été appliquées aux données concernées par ladite violation de sécurité.

Selon le règlement de 2013, les données sont considérées comme incompréhensibles si :

1. elles ont été cryptées en mode sécurisé à l'aide d'un algorithme normalisé et la clé utilisée pour les décrypter n'a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser ou
2. elles ont été remplacées par leur valeur hachée, calculée à l'aide d'une fonction de hachage normalisée à clé cryptographique, et la clé utilisée pour les hacher n'a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser.

Les fournisseurs doivent tenir à jour un inventaire des violations de données à caractère personnel (article 4 de la directive 2002/58/CE qui en définit le contenu de façon exhaustive).

Les informations fournies à l'abonné/particulier concernant la violation doivent se limiter à celle-ci et ne pas être associées à des informations concernant autre chose. Par exemple, faire figurer des informations concernant une violation de données à caractère personnel sur une facture courante ne devrait pas être considéré comme un moyen approprié de notifier une telle violation.

Les fournisseurs devraient mettre en œuvre les mesures techniques et d'organisation appropriées pour prévenir, détecter et empêcher les violations de données à caractère personnel. Les fournisseurs doivent examiner tout risque pouvant subsister après la réalisation de contrôles afin de comprendre où les violations de données à caractère personnel sont susceptibles de se produire.

Lorsque, pour fournir une partie du service de communications électroniques, il est fait appel à un autre fournisseur qui n'est pas directement lié par contrat avec les abonnés, cet autre fournisseur informe immédiatement celui qui l'a engagé en cas de violation de données à caractère personnel.

D. Les Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail « Article 29 » a publié des Lignes directrices en rapport en la matière (« *Guidelines on Personal data breach notification under Regulation* 2016/679 », Ref. WP 250 du 6 février 2018).

Fiche de guidance n° 27
Les autorités de contrôle indépendantes

Chapitre VI du RGPD (Articles 51 à 59)

Considérants 117 à 119, 121, 122, 124 à 131 du RGPD

A. Introduction

Les autorités de contrôle nationales conservent les missions qu'elles possédaient sous la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données :

- une mission de vérification de la bonne application des règles relatives à la protection des données personnelles ;
- une mission de sensibilisation du public et
- une mission d'accompagnement des responsables de traitement et des sous-traitants.

Ces compétences s'exerceront par principe sur le territoire de l'État membre dont l'autorité relève.

En revanche, la collaboration entre autorités de contrôle des données personnelles fait l'objet d'une organisation nouvelle, notamment en raison de l'instauration du mécanisme du guichet unique.

B. Statut d'indépendance

1. Obligation d'avoir au moins une autorité de contrôle de données personnelles par État membre

Chaque État membre doit prévoir qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du RGPD, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union.

Chaque autorité de contrôle contribue à l'application cohérente du RGPD dans l'ensemble de l'Union. À cette fin, les autorités de contrôle devront coopérer entre elles et avec la Commission européenne conformément au mécanisme de contrôle de la cohérence institué conformément au chapitre VII du RGPD.

Lorsqu'un État membre institue plusieurs autorités de contrôle, il devra désigner celle qui représente ces autorités auprès du comité européen de la protection des données (CEPD) et définir le mécanisme permettant de s'assurer du respect, par les autres autorités, des règles relatives au mécanisme de contrôle de la cohérence visé à l'article 63 du RGPD. Par exemple, en Allemagne, le contrôle des opérations de traitement des données à caractère personnel effectuées par le secteur non public est organisé par 16 entités, une pour chaque Länder allemand. L'Allemagne étant un pays fédéral, il existe aussi une autorité fédérale de contrôle.

2. Indépendance

Chaque autorité de contrôle devra exercer en toute indépendance les missions et les pouvoirs dont elle est investie conformément au RGPD.

Dans l'exercice de leurs missions et de leurs pouvoirs, le ou les membres de chaque autorité de contrôle demeurent libres de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent d'instructions de quiconque.

Le ou les membres de chaque autorité de contrôle s'abstiendront de tout acte incompatible avec leurs fonctions et, pendant la durée de leur mandat, n'exerceront aucune activité professionnelle incompatible, rémunérée ou non.

Chaque État membre veillera à ce que chaque autorité de contrôle :

- dispose des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, y compris lorsque celle-ci doit agir dans le cadre de l'assistance mutuelle, de la coopération et de la participation au CEPD ;

- choisisse et dispose de ses propres agents, qui sont placés sous les ordres exclusifs du ou des membres de l'autorité de contrôle concernée ;
- soit soumise à un contrôle financier qui ne menace pas son indépendance et qu'elle dispose d'un budget annuel public propre, qui peut faire partie du budget global national ou d'une entité fédérée.

3. Conditions générales applicables aux membres de l'autorité de contrôle

Les États membres prévoient que chacun des membres de leurs autorités de contrôle est nommé selon une procédure transparente par :

1. leur parlement ;
2. leur gouvernement ;
3. leur chef d'État ou
4. un organisme indépendant chargé de procéder à la nomination en vertu du droit de l'État membre.

Chaque membre a les qualifications, l'expérience et les compétences nécessaires, notamment dans le domaine de la protection des données à caractère personnel, pour l'exercice de ses fonctions et de ses pouvoirs.

Les fonctions d'un membre prennent fin à l'échéance de son mandat, en cas de démission ou de mise à la retraite d'office, conformément au droit de l'État membre concerné.

Un membre ne peut être démis de ses fonctions que s'il a commis une faute grave ou s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions.

4. Règles relatives à l'établissement de l'autorité de contrôle

Chaque État membre prévoit, par la loi, tous les éléments suivants :

1. la création de chaque autorité de contrôle ;
2. les qualifications et les conditions d'éligibilité requises pour être nommé membre de chaque autorité de contrôle ;
3. les règles et les procédures pour la nomination du ou des membres de chaque autorité de contrôle ;
4. la durée du mandat du ou des membres de chaque autorité de contrôle, qui ne peut être inférieure à quatre ans, sauf pour le premier mandat après le 24 mai 2016, dont une partie peut être d'une durée plus courte

lorsque cela est nécessaire pour protéger l'indépendance de l'autorité de contrôle au moyen d'une procédure de nominations échelonnées ;

5. le caractère renouvelable ou non du mandat du ou des membres de chaque autorité de contrôle et, si c'est le cas, le nombre de mandats ;
6. les conditions régissant les obligations du ou des membres et des agents de chaque autorité de contrôle, les interdictions d'activités, d'emplois et d'avantages incompatibles avec celles-ci, y compris après la fin de leur mandat, et les règles régissant la cessation de l'emploi.

Le ou les membres et les agents de chaque autorité de contrôle sont soumis, conformément au droit de l'Union européenne ou au droit des États membres, au secret professionnel concernant toute information confidentielle dont ils ont eu connaissance dans l'exercice de leurs missions ou de leurs pouvoirs, y compris après la fin de leur mandat. Pendant la durée de leur mandat, ce secret professionnel s'applique en particulier au signalement par des personnes physiques de violations du Règlement.

C. Compétence, missions et pouvoirs

1. Compétence

Chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au RGPD sur le territoire de l'État membre dont elle relève.

Lorsque le traitement est effectué par des autorités publiques ou des organismes privés agissant sur la base de l'article 6.1.c ou 6.1.e du RGPD, l'autorité de contrôle de l'État membre concerné est compétente.

Indépendance du pouvoir judiciaire oblige, les autorités de contrôle ne sont pas compétentes pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle.

2. Compétence de l'autorité de contrôle chef de file (traitements transfrontaliers)

L'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60 du RGPD.

Toutefois, chaque autorité de contrôle est compétente pour traiter une réclamation introduite auprès d'elle ou une éventuelle violation du RGPD, si son objet :

1. concerne uniquement un établissement dans l'État membre dont elle relève ou
2. affecte sensiblement des personnes concernées dans cet État membre uniquement.

Dans ce cas, l'autorité de contrôle informera sans tarder l'autorité de contrôle chef de file de la question.

Dans un délai de trois semaines suivant le moment où elle a été informée, l'autorité de contrôle chef de file décide si elle traitera ou non le cas conformément à la procédure de coopération prévue à l'article 60 du RGPD, en considérant s'il existe ou non un établissement du responsable du traitement ou du sous-traitant dans l'État membre de l'autorité de contrôle qui l'a informée.

- Si l'autorité de contrôle chef de file décide de traiter le cas, la procédure de coopération du RGPD s'applique (article 60). L'autorité de contrôle qui a informé l'autorité de contrôle chef de file peut lui soumettre un projet de décision. L'autorité de contrôle chef de file tient le plus grand compte de ce projet lorsqu'elle élabore le projet de décision visé à l'article 60.3 du RGPD.
- Lorsque l'autorité de contrôle chef de file décide de ne pas traiter le cas, l'autorité de contrôle qui l'a informée le traite conformément aux articles 61 (« Assistance mutuelle ») et 62 (« Opérations conjointes »).

L'autorité de contrôle chef de file est le seul interlocuteur du responsable du traitement ou du sous-traitant pour le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant.

3. Missions des autorités de contrôle

Sans préjudice des autres missions prévues dans le RGPD, chaque autorité de contrôle, sur son territoire, :

1. contrôle l'application du RGPD et veille au respect de celui-ci par les responsables du traitement.

   L'autorité de contrôle encouragera aussi la sensibilisation des responsables du traitement et des sous-traitants en ce qui concerne les obligations qui leur incombent en vertu du RGPD ;
2. effectue des enquêtes sur l'application du RGPD, y compris sur la base d'informations reçues d'une autre autorité de contrôle ou d'une autre autorité publique ;
3. favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement.

Les activités destinées spécifiquement aux personnes vulnérables comme les enfants sont censées faire l'objet d'une attention particulière ;

4. fournit, sur demande, à toute personne concernée des informations sur l'exercice des droits que lui confère le RGPD et, si nécessaire, coopère, à cette fin, avec les autorités de contrôle d'autres États membres ;
5. traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association, examine l'objet de la réclamation et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire. Chaque autorité de contrôle devra faciliter l'introduction des réclamations par des mesures telles que la fourniture d'un formulaire de réclamation qui peut aussi être rempli par voie électronique, sans que d'autres moyens de communication ne soient exclus ;
6. conseille, conformément au droit de leur État, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement.

   Dès lors, cela reviendra-il à dire que les autorités de contrôle seront à chaque fois consulter obligatoirement lorsqu'une loi concernant la protection des données personnelles au sens large est déposée au parlements nationaux (ou fédéraux) ? Nous l'espérons ;
7. coopère avec d'autres autorités de contrôle, y compris en partageant des informations, et fournit une assistance mutuelle dans ce cadre en vue d'assurer une application cohérente du RGPD et des mesures prises pour en assurer le respect ;
8. établit et tient à jour une liste en lien avec l'obligation d'effectuer une AIPD en application de l'article 35.4 du RGPD.

   L'autorité de protection peut aussi établir une liste reprenant les activités de traitement pour lesquelles un AIPD n'est pas obligatoire ;
9. fournit des conseils sur les opérations de traitement qui sont susceptibles de constituer une violation du RGPD (art. 36.2 du RGPD) ;
10. adopte les clauses contractuelles types visées à l'article 28.8, et à l'article 46.2.d du RGPD ;
11. autorise les clauses contractuelles et les dispositions visées à l'article 46.3 du RGPD ainsi que les règles d'entreprise contraignantes en application de l'article 47 du RGPD ;
12. tient des registres internes des violations au RGPD et des mesures correctrices prises conformément à l'article 58.2 du RGPD ;
13. encourage l'élaboration de codes de conduite, rend un avis et approuve les codes de conduite qui fournissent des garanties suffisantes ;

14. procède, le cas échéant, à l'examen périodique des certifications délivrées (art. 42.7 du RGPD) ;
15. encourage la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données et approuve les critères de certification ;
16. rédige et publie les critères d'agrément d'un organisme chargé du suivi des codes de conduite en application de l'article 41 et d'un organisme de certification en application de l'article 43 du RGPD ;
17. procède à l'agrément d'un organisme chargé du suivi des codes de conduite en application de l'article 41 et d'un organisme de certification en application de l'article 43 du RGPD ;
18. contribue aux activités du CEPD ;
19. suit les évolutions pertinentes, dans la mesure où ces évolutions ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et de la communication et des pratiques commerciales ;
20. s'acquitte de toute autre mission relative à la protection des données à caractère personnel (clause résiduelle ou clause fourre-tout).

L'accomplissement des missions de chaque autorité de contrôle est gratuit pour la personne concernée et, le cas échéant, pour le DPD.

Lorsque les demandes sont manifestement infondées ou excessives, en raison, notamment, de leur caractère répétitif, l'autorité de contrôle peut exiger le paiement de frais raisonnables basés sur les coûts administratifs ou refuser de donner suite à la demande. Il incombe à l'autorité de contrôle de démontrer le caractère manifestement infondé ou excessif de la demande.

4. Pouvoirs d'enquête, mesures correctrices, pouvoirs d'autorisation et pouvoirs consultatifs des autorités de protection de données personnelles

a. *Pouvoirs d'enquête*

Chaque autorité de contrôle dispose de tous les pouvoirs d'enquête suivants :

1. ordonner au responsable du traitement et au sous-traitant, et, le cas échéant, au représentant du responsable du traitement ou du sous-traitant, de lui communiquer toute information dont elle a besoin pour l'accomplissement de ses missions ;
2. mener des enquêtes sous la forme d'audits sur la protection des données ;
3. procéder à un examen des certifications ;

4. notifier au responsable du traitement ou au sous-traitant une violation alléguée du RGPD ;
5. obtenir du responsable du traitement et du sous-traitant l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'accomplissement de ses missions ;
6. obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation et à tout moyen de traitement, conformément au droit de l'Union ou au droit procédural des États membres.

b. *Mesures correctrices*

Chaque autorité de contrôle dispose du pouvoir d'adopter toutes les mesures correctrices suivantes :

1. avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du RGPD ;
2. rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du RGPD ;
3. ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du RGPD ;
4. ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du RGPD, le cas échéant, de manière spécifique et dans un délai déterminé ;
5. ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel ;
6. imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ;
7. ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement (art. 16, 17 et 18 du RGPD) et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17.2 et de l'article 19 du RGPD ;
8. retirer une certification ou ordonner à l'organisme de certification de retirer une certification ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites ;

9. imposer une amende administrative en application de l'article 83 du RGPD, en complément ou à la place des mesures correctrices, en fonction des caractéristiques propres à chaque cas ;
10. ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.

c. *Pouvoirs d'autorisation et pouvoirs consultatifs*

Chaque autorité de contrôle dispose de tous les pouvoirs d'autorisation et de tous les pouvoirs consultatifs suivants :

1. conseiller le responsable du traitement lorsque celui-ci doit consulter une autorité de contrôle de données personnelles pour finaliser une AIPD ;
2. émettre, de sa propre initiative ou sur demande, des avis à l'attention du parlement national, du gouvernement de l'État membre ou, conformément au droit de l'État membre, d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel ;
3. autoriser le traitement visé à l'article 36.5 du RGPD, si le droit de l'État membre exige une telle autorisation préalable ;
4. rendre un avis sur les projets de codes de conduite et les approuver (art. 40.5 du RGPD) ;
5. agréer des organismes de certification ;
6. délivrer des certifications et approuver des critères de certification (art. 42.5 du RGPD) ;
7. adopter les clauses types de protection des données visées à l'article 28.8 et à l'article 46.2.d du RGPD ;
8. autoriser les clauses contractuelles visées à l'article 46.3.a du RGPD ;
9. autoriser les arrangements administratifs visés à l'article 46.3.b du RGPD ;
10. approuver les règles d'entreprise contraignantes (art. 47 du RGPD).

L'exercice des pouvoirs conférés à l'autorité de contrôle est subordonné à des garanties appropriées, y compris le droit à un recours juridictionnel effectif et à une procédure régulière, prévues par le droit de l'Union et le droit des États membres conformément à la Charte des droits fondamentaux.

Chaque État membre prévoit, par la loi, que son autorité de contrôle a le pouvoir de porter toute violation du RGPD à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du RGPD.

Chaque État membre peut prévoir, par la loi, que son autorité de contrôle dispose de pouvoirs additionnels. L'exercice de ces pouvoirs n'entrave pas le bon fonctionnement du chapitre VII « Coopération et cohérence ».

5. Rapports d'activité

Chaque autorité de contrôle établit un rapport annuel sur ses activités, qui peut comprendre une liste des types de violations notifiées et des types de mesures correctrices.

Ces rapports sont transmis au parlement national, au gouvernement et à d'autres autorités désignées par le droit de l'État membre. Ils sont mis à la disposition du public, de la Commission européenne et du CEPD.

D. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 28 : L'identification de l'autorité de contrôle chef de file en cas de transferts transfrontaliers (le guichet unique ou le « one-stop-shop »)*
- *Fiche de guidance n° 29 : La bonne coopération entre les autorités de contrôle des données personnelles*
- *Fiche de guidance n° 30 : Le mécanisme de contrôle de la cohérence*
- *Fiche de guidance n° 31 : Le CEPD (le « Comité européen de la protection des données »)*
- *Fiche de guidance n° 33 : Les sanctions et leur caractère dissuasif*

Fiche de guidance n° 28

L'identification de l'autorité de contrôle chef de file en cas de transferts transfrontaliers (le guichet unique ou le « *one-stop-shop* »)

Articles 4.23 & 56 du RGPD

Considérants 27, 28, 31 & 34, 124 à 131 du RGPD

A. Principe

Les entreprises multinationales qui opèrent des traitements de données dans différents États pourront fonctionner avec une seule autorité de contrôle « chef de file ». Cette autorité travaillera toutefois en étroite coopération avec ses homologues également potentiellement concernées par les traitements notamment parce que des données de leurs citoyens sont traitées.

En effet, selon le principe de l'autorité de contrôle chef de file (« *lead authority principle* »), la supervision des traitements transfrontaliers devra être réalisée par uniquement une et une seule autorité de contrôle européenne. Dès lors, l'autorité chef de file sera le seul interlocuteur du responsable du traitement et du sous-traitant.

Toutefois, le Règlement européen maintiendra une compétence résiduelle des autres autorités de contrôle dans un cas de figure. Chaque autorité de contrôle nationale demeurera compétente pour connaître d'une réclamation introduite auprès d'elle si son objet ne vise qu'un établissement situé dans l'État membre dont elle dépend ou en cas d'infraction au Règlement si celle-ci n'affecte que les personnes concernées dans l'État membre dont elle dépend.

L'autorité chef de file devra être informée de cette réclamation ou infraction au Règlement et pourra ensuite décider de gérer ou non le cas.

La concrétisation de l'objectif voulu (« clarifier la situation en cas de traitements transfrontaliers ») est bien compliquée à comprendre.

Tentons d'y voir plus clair.

B. Quand avons-nous un traitement transfrontalier ?

Selon l'article 4.23 du RGPD, il y aura un « traitement transfrontalier » (un « *cross-border processing* »), lorsque :

1. un traitement de données à caractère personnel a lieu dans l'Union européenne dans le cadre des activités d'établissements situés
   i. dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant *et*
   ii. lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres

   (par exemple, lorsqu'une société à des établissements tant en France qu'en Roumanie et que les traitements ont lieu dans ces deux pays)

   ou
2. un traitement de données à caractère personnel a lieu dans l'Union européenne dans le cadre des activités
   i. d'un établissement unique d'un responsable du traitement ou d'un sous-traitant
   ii. qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres

   (par exemple, une société située en Belgique réalise des traitements qui affectent sensiblement des Français et des Hongrois).

Si une de ces deux situations se produit, il est nécessaire d'identifier l'autorité de contrôle chef de file qui va devoir gérer les questions relatives à ces traitements transfrontaliers.

L'interprétation du fait de savoir si l'une de ces deux situations se produit ou pas se fera au fil du temps par les autorités de contrôle des données personnelles.

Notons que les notions de « affecter sensiblement » ou « susceptible d'affecter sensiblement » sont censées exclure des traitements transfrontaliers ceux ayant peu ou aucun effet sur les individus d'un autre État Membre. D'après les lignes directrices adoptées par le Groupe de Travail « Article 29 », l'expression « affecte sensiblement », non définie dans le règlement, doit être interprétée au

cas par cas, en prenant en compte le contexte du traitement, le type de données, l'objet du traitement et certains autres facteurs comme les possibles dommages que le traitement peut causer, les effets probables sur les droits, etc.

C. Identification de l'autorité de contrôle chef de file

1. Principe

Déterminer l'autorité chef de file va dépendre de la détermination correcte de la localisation du principal établissement ou de l'établissement unique du responsable de traitement ou du sous-traitant dans l'UE. En effet, c'est l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement qui sera compétente pour agir en tant qu'autorité de contrôle chef de file.

Selon l'article 4.16 du RGPD, l'« établissement principal » se définit comme :

1. en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale (son siège social) dans l'Union européenne,

   à moins que les décisions quant aux finalités et aux moyens d'un traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union *et*

   que ce dernier établissement a le pouvoir de faire appliquer ces décisions,

   => auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal pour ce traitement

   => à voir dès lors, si, dans certaines hypothèses, plusieurs autorités chef de file peuvent/doivent être identifiées ;

2. en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union

   ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du RGPD.

2. Identification de l'autorité de contrôle chef de file pour un responsable de traitement

Première étape : identification du lieu où se situe l'administration centrale du responsable du traitement.

Il s'agit du lieu où les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel sont prises et du lieu où se trouve l'organe qui a le pouvoir de faire appliquer ces décisions.

Il s'ensuit qu'il pourrait y avoir des situations où plus d'une autorité de contrôle chef de file pourraient être identifiées. Par exemple, dans les situations où une multinationale décide d'avoir plusieurs centres de décision, dans différents pays et ce pour plusieurs catégories d'activités de traitements différents.

Deuxième étape : Quid si l'établissement principal ne correspond pas au lieu où se trouve l'administration centrale de l'établissement ?

C'est au responsable de traitement lui-même à déterminer où se situe l'établissement principal et donc quelle est son autorité de contrôle chef de file. Toutefois, cette décision pourra être révisée par les autorités de contrôle des données personnelles après coup, le RGPD ne permettant pas le forum shopping.

Dans le cas où l'établissement principal et central ne se situent pas au même endroit dans l'UE, plusieurs éléments entrent en considération afin de pouvoir adéquatement déterminer où se situe l'établissement principal du responsable de traitement :

- où se situe l'endroit où les décisions sur les finalités et les moyens relatifs aux traitements reçoivent le « *final sign off* » (l'accord final) du responsable du traitement ?
- où se prennent les décisions à propos des activités commerciales qui impliquent des traitements de données personnelles ?
- où se situe le pouvoir de prendre des décisions finales ?
- où se trouve le dirigeant (ou les dirigeants) qui a des responsabilités générales à propos des traitements transfrontaliers ?
- dans le cas où la société a été enregistrée dans un seul territoire, où se situe cet enregistrement/immatriculation ?

Dans le cas d'un groupe de sociétés, le lieu où se situe la société-mère ou le centre opérationnel du groupe correspond généralement au lieu où se situe son administration centrale. Dès lors, ce sera le lieu où se situe la société-mère qui sera considéré comme l'établissement principal du groupe de sociétés. Attention toutefois aux groupes de sociétés qui permettent à leurs filiales d'avoir un réel pouvoir d'indépendance par rapport à des décisions sur des activités impliquant des traitements de données à caractère personnel. Dans ce cas-là, pour le traitement pour lequel la filiale a une indépendance de décision, la décision risque d'être différente.

Dans le cas de responsables de traitements conjoints, ils devront déterminer ensemble où se situe l'établissement des responsables conjoints qui aura le pouvoir d'implémenter les décisions relatives aux traitements des données pour l'ensemble des responsables concernés. Cet établissement sera dès lors à considérer comme étant l'établissement principal pour les traitements réalisés dans le cadre et pour le compte de leur accord.

Quid lorsque des traitements transfrontaliers sont effectués par un responsable du traitement établi dans plusieurs États membres mais qui n'a aucun établissement central situé en Europe car aucun de ses établissements européens ne prend réellement les décisions finales à propos desdits traitements (= les décisions sont donc prises exclusivement en-dehors de l'UE) ?

Ce sera à la société elle-même à déterminer l'établissement qui implémente les décisions relatives aux traitements et qui prendra dès lors la responsabilité en rapport avec les traitements. De plus, dans le cas où une société ne possède aucun établissement dans l'UE, la simple présence d'un représentant ne permet pas d'actionner le système du one-stop-shop.

Cela signifie que les responsables de traitement qui n'ont aucun établissement dans l'UE auront à traiter avec les autorités de contrôle de chaque État membre dans lesquels ils sont actifs et ce grâce au travers de leur représentant local.

3. Identification de l'autorité chef de file pour un sous-traitant

Le système du « *one-stop-shop* » est aussi présent dans le RGPD au bénéfice des sous-traitants. En effet, nous avons vu que le RGPD impose dorénavant des obligations à charge des sous-traitants.

Que se passe-t-il dès lors lorsque le sous-traitant a plusieurs établissements dans plusieurs États membres ?

La logique est la même que pour un responsable de traitement.

En effet, ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son établissement principal sera le lieu de son établissement central. Ce sous-traitant sera sous la gouverne de l'autorité de contrôle qui y est territorialement compétente.

Dans le cas où ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, le lieu de son établissement principal sera le lieu où se déroule l'essentiel de ses activités de traitement.

Toutefois, dans le cas où les situations impliquent tant un responsable du traitement et un sous-traitant, l'autorité de contrôle chef de file sera l'autorité de contrôle du responsable de traitement (considérant 36 du RGPD) sauf dans le cas où le responsable du traitement n'est pas situé dans l'UE.

Il peut arriver qu'un sous-traitant exerce ses activités pour des responsables de traitements situés dans plusieurs États membres.

Prenons l'exemple d'un fournisseur de services dans le cloud.

Dans une telle situation, nous venons de le voir, l'autorité de contrôle chef de file sera l'autorité de contrôle du responsable de traitement. Dès lors, cela signifie qu'un tel sous-traitant aura affaire avec plusieurs autorités de contrôle chef de file s'il traite avec plusieurs responsables de traitement européens.

D. Lignes directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail « Article 29 » a adopté, le 5 avril 2017, des lignes directrices en rapport avec la détermination de l'autorité chef de file.

Les lignes directrices sont disponibles dans toutes les langues de l'Union européenne via le site internet du Groupe de Travail (« Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant », Réf. WP 244 rev.01).

E. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 27 : Les autorités de contrôle indépendantes*
- *Fiche de guidance n° 29 : La bonne coopération entre les autorités de contrôle des données personnelles*
- *Fiche de guidance n° 30 : Le mécanisme de contrôle de la cohérence*
- *Fiche de guidance n° 31 : Le CEPD (le « Comité européen de la protection des données »)*

Fiche de guidance n° 29

La bonne coopération entre les autorités de contrôle des données personnelles

Articles 60 à 62 du RGPD

Considérants 5, 133 & 134 du RGPD

A. Introduction

Le RGPD prévoit des mécanismes et des procédures afin de favoriser la coopération entre les autorités de contrôle des données personnelles dans le but de favoriser une interprétation cohérente au niveau européen des règles issues du RGPD.

Le RGPD a ainsi créé le Comité européen de la protection des données (le CEPD ou « *European Data Protection Board* », EDPB en anglais) (futur remplaçant du Groupe de Travail « Article 29 »).

B. Les mesures mises en place pour favoriser la coopération entre l'autorité chef de file et les autres autorités de contrôle

Le RGPD prévoit d'une part, une obligation pour les autorités de contrôle de coopérer entre elles, d'autre part, de se prêter mutuellement assistance.

En effet, le Règlement permet dorénavant aux autorités de contrôle de réaliser ensemble des opérations conjointes comme des enquêtes ou des contrôles à propos de l'application d'une mesure par un responsable du traitement ou un sous-traitant établi dans un autre État membre.

1. L'obligation de coopérer ensemble (art. 61 du RGPD)

Supposons qu'une réclamation ait été introduite auprès d'une autorité de contrôle qualifiée d'autorité chef de file. L'autorité de contrôle se rend compte que la réclamation soulève une question aux implications transfrontières.

Elle peut, dans ce cas, requérir la coopération des autres autorités de contrôle concernées.

Le RGPD prévoit dans ce cas l'ensemble de la procédure de coopération à appliquer.

a. *La décision par consensus des autorités de protection*

La coopération a pour objectif de parvenir à un consensus entre les différentes autorités de contrôle grâce aux informations qu'elles vont devoir s'échanger. Les communications entre les différentes autorités de contrôle devront se réaliser par voie électronique et au moyen d'un formulaire type.

La procédure en tant que telle est assez complexe.

L'autorité de contrôle chef de file devra tout d'abord communiquer (« sans tarder » précise le RGPD) les informations utiles sur la question concernée aux autres autorités de contrôle concernées.

Le RGPD définit ce qu'il faut entendre par « autorité de contrôle concernée » (art. 4.22 du RGPD).

Une autorité de contrôle concernée est une « autorité de contrôle concernée par un traitement de données à caractère personnel dans le cas où :

- le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève ;
- des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être ou
- une réclamation a été introduite auprès de cette autorité de contrôle. ».

Ce sera donc à l'autorité de contrôle chef de file à déterminer, en s'aidant de cette définition, les autres autorités de protection qui sont utiles à la résolution de sa ou de ses questions.

Suite au retour des autres autorités de contrôle, l'autorité de contrôle chef de file devra soumettre (à nouveau « sans tarder ») un projet de décision aux autres autorités de contrôle concernées en vue d'obtenir leur avis sur son projet de décision. Ce projet de décision devra tenir dûment compte de leur point de vue et donc des informations que les autres autorités avaient préalablement échangées.

Le RGPD précise par après que :

> « Dans le cas où une des autres autorités de contrôle concernées formule, dans un délai de quatre semaines après avoir été consultée, une objection pertinente et

motivée à l'égard du projet de décision, l'autorité de contrôle chef de file, si elle ne suit pas l'objection pertinente et motivée ou si elle est d'avis que cette objection n'est pas pertinente ou motivée, soumet la question au mécanisme de contrôle de la cohérence de l'article 63 ».

Dès lors, après avoir reçu de la part de l'autorité chef de file le projet de décision, une autorité de contrôle concernée peut ne rien dire et en quelque sorte acquiescer au projet de décision de l'autorité chef de file.

Elle peut aussi formuler une objection pertinente et motivée à l'égard du projet de décision. Elle devra obligatoirement formuler ses objections dans un délai de quatre semaines après avoir été consultée par l'autorité chef de file.

L'autorité chef de file peut décider de suivre les objections reçues. Dans ce cas, elle devra soumettre aux autres autorités de contrôle concernées consultées un projet de décision révisé en vue d'obtenir leur avis à nouveau. Les autorités concernées ont deux semaines pour réagir (si elles le souhaitent bien sûr). Si l'autorité chef de file conteste ces nouvelles objections, elle devra soumettre le dossier au mécanisme de cohérence impliquant l'intervention du comité européen de la protection des données (le CEPD).

Lorsqu'aucune des autres autorités de contrôle concernées consultées par l'autorité chef de file n'a formulé d'objection à l'égard du projet de décision soumis par l'autorité de contrôle chef de file dans les délais soit de quatre semaines, soit de deux semaines, l'autorité de contrôle chef de file et les autorités de contrôle concernées sont réputées approuver ce projet de décision. L'ensemble de ces autorités de protection seront liées par cette décision.

L'autorité de contrôle chef de file devra formellement adopter la décision, la notifier à l'établissement principal ou à l'établissement unique du responsable du traitement ou du sous-traitant concerné par la question. Elle devra aussi informer les autres autorités de contrôle concernées et le CEPD de la décision en question, y compris en communiquant un résumé des faits et motifs pertinents.

Tout n'est pas fini pour autant.

b. *Gestion de la réclamation initiale*

L'autorité de contrôle auprès de laquelle la réclamation a été introduite devra informer l'auteur de la réclamation de la suite de son dossier et de la décision intervenue entre les autorités de contrôle.

Trois hypothèses peuvent se produire :

1. dans le cas où l'autorité de contrôle accepte la réclamation, elle devra informer l'auteur de la réclamation de la décision qui est intervenue entre les diverses autorités de contrôle ;
2. lorsque la réclamation est refusée ou rejetée, l'autorité de contrôle auprès de laquelle ladite réclamation a été introduite adopte la décision, la notifie à l'auteur de la réclamation et en informe le responsable du traitement ;

3. lorsque l'autorité de contrôle chef de file et les autorités de contrôle concernées sont d'accord pour refuser ou rejeter certaines parties de la réclamation et donner suite à d'autres parties de cette réclamation, une décision distincte est adoptée pour chacune des parties de la réclamation.

   L'autorité de contrôle chef de file adopte la décision pour la partie relative aux actions concernant le responsable du traitement, la notifie à l'établissement principal ou à l'établissement unique du responsable du traitement ou du sous-traitant sur le territoire de l'État membre dont elle relève et en informe l'auteur de la réclamation. L'autorité de contrôle de l'auteur de la réclamation adopte la décision pour la partie concernant le refus ou le rejet de cette réclamation, la notifie à cette personne et en informe le responsable du traitement ou le sous-traitant.

Après avoir été informé de la décision de l'autorité de contrôle chef de file, le responsable du traitement ou le sous-traitant prend les mesures nécessaires pour assurer le respect de cette décision en ce qui concerne les activités de traitement menées dans le cadre de tous ses établissements dans l'Union européenne. Le responsable du traitement ou le sous-traitant notifie les mesures prises pour assurer le respect de la décision à l'autorité de contrôle chef de file, qui en informera les autres autorités de contrôle concernées.

Lorsque, dans des circonstances exceptionnelles, une autorité de contrôle concernée a des raisons de considérer qu'il est urgent d'intervenir pour protéger les intérêts des personnes concernées, la procédure d'urgence visée à l'article 66 du RGPD s'applique.

2. L'obligation de se prêter mutuellement assistance (art. 62)

Les autorités de contrôle doivent de se prêter mutuellement assistance en vue de mettre en œuvre et d'appliquer le RGPD de façon cohérente.

Pour ce faire, le RGPD prévoit que les autorités de contrôle doivent se communiquer toutes les informations utiles et mettre en place des mesures pour coopérer efficacement.

L'assistance mutuelle pourra concerner de multiples sujets notamment :

1. des demandes d'informations et
2. des mesures de contrôle comme des demandes d'autorisation et de consultation préalables, des inspections et des enquêtes.

Chaque autorité de contrôle européenne devra prendre toutes les mesures appropriées requises pour être capable de répondre à une demande d'une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception d'une telle demande.

Elle pourrait par exemple transmettre des informations utiles sur la conduite d'une enquête qui a rapport à la demande.

L'autorité de contrôle requise informe l'autorité de contrôle requérante des résultats obtenus ou, selon le cas, de l'avancement des mesures prises pour donner suite à la demande.

Les demandes d'assistances devront contenir toutes les informations nécessaires pour pouvoir y répondre adéquatement, notamment la finalité et les motifs de la demande. Le Règlement précise que les « informations échangées ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées ».

Une autorité de contrôle requise devra aider l'autre autorité de contrôle dans tous les cas de figure.

Toutefois, elle pourrait refuser son aide si :

1. elle estime n'être pas compétente pour traiter l'objet de la demande ou pour prendre les mesures requises ou
2. satisfaire à la demande constituerait dans son chef une violation du RGPD ou du droit de l'Union ou de son droit national.

L'autorité de contrôle requise devra expliquer à l'autre autorité les raisons de tout refus de satisfaire à une demande.

En règle générale, les autorités de contrôle requises communiqueront entre elles par voie électronique et au moyen de formulaires type.

Les autorités de contrôle requises ne perçoivent pas de frais pour toute action qu'elles prennent à la suite d'une demande d'assistance mutuelle. Elles peuvent toutefois convenir de règles concernant l'octroi de dédommagements entre elles pour des dépenses spécifiques résultant de la fourniture d'une assistance mutuelle et ce dans des circonstances exceptionnelles.

Lorsqu'une autorité de contrôle ne fournit pas les informations demandées dans le délai d'un mois :

1. l'autorité de contrôle requérante retrouve une possibilité d'action. Elle pourra dans ce cas adopter une mesure provisoire mais qui ne vaudra que sur son territoire national. Une autorité de contrôle qui fait donc appel à l'assistance mutuelle peut adopter une mesure provisoire si elle ne reçoit pas de réponse à sa demande d'assistance mutuelle dans un délai d'un mois à compter de la réception de la demande d'assistance mutuelle par l'autre autorité de contrôle ;
2. les circonstances permettant de considérer qu'il est urgent d'intervenir conformément à l'article 66.1 du RGPD sont dès lors réputées réunies nécessitant une décision contraignante d'urgence du CEPD en application de l'article 66.2 du RGPD.

La Commission européenne pourra, par voie d'actes d'exécution, préciser la forme et les procédures de l'assistance mutuelle, ainsi que les modalités de l'échange d'informations par voie électronique entre les autorités de contrôle et entre les autorités de contrôle et le comité, notamment en ce qui concerne les formulaires type.

3. La faculté de mener des opérations conjointes (art. 63 du RGPD)

Les autorités de contrôle peuvent réaliser des opérations conjointes impliquant la participation de membres ou d'agents des autorités de contrôle de plusieurs États membres.

Ces opérations conjointes peuvent être des enquêtes conjointes menant le cas échéant à des mesures répressives conjointes.

a. *Qui peut participer à ces opérations conjointes ?*

Les opérations conjointes vont concerner deux sortes de traitements :

1. ceux mis en place par un responsable du traitement ou par un sous-traitant qui est établi dans plusieurs États membres (première hypothèse) et
2. ceux qui sensiblement affectent un nombre important de personnes concernées dans plusieurs États membres (seconde hypothèse).

L'opération conjointe va devoir impliquer plusieurs autorités de protection.

Lesquelles ?

Ce seront les autorités de protection dont relèvent les responsables de traitement ou sous-traitants en fonction de la première ou seconde hypothèse présentées ci-dessus.

Chacune a le droit de participer aux opérations conjointes.

L'autorité de contrôle chef de file pour le traitement concerné par l'opération conjointe sera l'autorité de contrôle qui va diriger ladite opération. Elle sera qualifiée d'autorité de contrôle d'accueil par opposition aux autres autorités qui seront qualifiées d'autorités d'origine.

L'autorité d'accueil va devoir inviter les autorités de contrôle concernées (ou d'origine) à prendre part aux opérations conjointes concernées et donner suite sans tarder à toute demande d'une autorité de contrôle souhaitant y participer.

L'autorité de contrôle d'accueil peut, conformément au droit d'un État membre (de quel État membre s'agit-il ici ? le RGPD ne le précise pas mais on suppose qu'il s'agira du droit dont elle relève) et avec l'autorisation de l'autorité de contrôle d'origine, conférer des pouvoirs, notamment des pouvoirs d'enquête, aux membres ou aux agents de l'autorité de contrôle d'origine participant à des opérations conjointes.

L'autorité d'accueil peut aussi accepter, pour autant que son droit le permette, que les membres ou les agents de l'autorité de contrôle d'origine exercent leurs pouvoirs d'enquête conformément à leur droit national. Ces pouvoirs d'enquête ne peuvent être exercés que sous l'autorité et en présence de membres ou

d'agents de l'autorité de contrôle d'accueil. Les membres ou agents de l'autorité de contrôle d'origine sont soumis au droit de l'État membre de l'autorité de contrôle d'accueil.

Lorsque les agents de l'autorité de contrôle d'origine opèrent dans un autre État membre dans le cadre d'une opération conjointe, l'État membre dont relève l'autorité de contrôle d'accueil assume la responsabilité de leurs actions, y compris la responsabilité des dommages qu'ils causent au cours des opérations dont ils sont chargés.

Dans le cas où des dommages ont été réalisés lors d'une opération conjointe, l'État membre sur le territoire duquel des dommages ont été causés répare ces dommages selon les conditions applicables aux dommages causés par ses propres agents. L'État membre dont relève l'autorité de contrôle d'origine dont les agents ont causé des dommages à des personnes sur le territoire d'un autre État membre rembourse intégralement à cet autre État membre les sommes qu'il a versées aux ayants droit.

Toutefois, un État membre devra s'abstenir de demander à un autre État membre que l'État membre d'origine le remboursement lié aux dommages causés par des agents de l'autorité de contrôle d'origine qui ont opéré sur son territoire. L'État membre en question peut toutefois toujours exercer tous ses droits à l'égard des tiers.

Dans le cas où une opération conjointe est envisagée et qu'une autorité de contrôle ne répond pas, dans un délai d'un mois, à l'invitation de prendre part à une opération conjointe :

1. d'une part, les autres autorités de contrôle peuvent adopter une mesure provisoire sur le territoire de l'État membre dont celle-ci relève conformément à l'article 55 du RGPD ;
2. d'autre part, les circonstances permettant de considérer qu'il est urgent d'intervenir conformément à l'article 66.1, sont présumées être réunies. Il est dès lors possible de saisir le CEPD en application de l'article 66.2 du RGPD pour obtenir de sa part un avis ou une décision contraignante d'urgence.

C. Les traitements locaux

Chaque autorité de contrôle qui ne fait pas office d'autorité de contrôle chef de file devrait être compétente pour traiter les cas de portée locale.

Un traitement est local lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres mais que l'objet du traitement spécifique ne se rapporte qu'à un traitement effectué dans un seul État membre et ne porte que sur des personnes concernées de ce seul État membre.

Par exemple lorsqu'il s'agit de traiter des données à caractère personnel relatives à des employés dans le contexte des relations de travail propre à un État membre

Dans ce cas, l'autorité de contrôle devrait informer sans tarder l'autorité de contrôle chef de file de la question. Après avoir été informée, l'autorité de contrôle chef de file devra décider si elle traitera le cas en vertu de la disposition relative à la coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées, ou si l'autorité de contrôle qui l'a informée pourra traiter le cas au niveau local.

Dans le contexte de son appréciation, l'autorité de contrôle chef de file devrait regarder s'il existe un établissement du responsable du traitement ou du sous-traitant dans l'État membre dont relève l'autorité de contrôle qui l'a informée, afin d'assurer l'exécution effective d'une décision à l'égard du responsable du traitement ou du sous-traitant.

Lorsque l'autorité de contrôle chef de file décide de traiter le cas, l'autorité de contrôle qui l'a informée pourra lui soumettre un projet de décision, dont l'autorité de contrôle chef de file devrait tenir le plus grand compte lorsqu'elle élaborera son projet de décision dans le cadre du mécanisme de guichet unique.

De plus, chaque autorité de contrôle sera compétente sur le territoire de l'État membre dont elle relève pour exercer les missions et les pouvoirs dont elle est investie conformément au RGPD.

En effet, lorsque le traitement est effectué par des autorités publiques ou des organismes privés agissant sur la base de l'article 6.1.c ou 6.1.e du RGPD uniquement l'autorité de contrôle de l'État membre concerné est compétente.

Cela devrait couvrir, notamment, le traitement affectant des personnes concernées sur le territoire de l'État membre dont elle relève ou le traitement des réclamations introduites par les personnes concernées, la conduite d'enquêtes sur l'application du règlement et la sensibilisation du public aux risques, règles, garanties et droits liés au traitement des données à caractère personnel.

D. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 27 : Les autorités de contrôle indépendantes*
- *Fiche de guidance n° 28 : L'identification de l'autorité de contrôle chef de file en cas de transferts transfrontaliers (le guichet unique ou le « one-stop-shop »)*
- *Fiche de guidance n° 30 : Le mécanisme de contrôle de la cohérence*
- *Fiche de guidance n° 31 : Le CEPD (le « Comité européen de la protection des données »)*

Fiche de guidance n° 30
Le mécanisme de contrôle de la cohérence

Articles 63 à 67 du RGPD

Considérants 135 à 138 167 à 169 du RGPD

A. Introduction

Afin de contribuer à l'application cohérente du RGPD dans l'ensemble de l'Union européenne, les autorités de contrôle devront coopérer entre elles et, le cas échéant, avec la Commission européenne dans le cadre du mécanisme de contrôle de la cohérence établi par le RGPD.

Le comité européen de la protection des données (le CEPD) établi par le RGPD va remplacer à partir du 25 mai 2018 le Groupe de Travail « Article 29 ».

Le CEPD va jouer un rôle central dans l'harmonisation de la matière au niveau européen. Il aura principalement deux rôles : celui de donner un avis concernant des décisions que veulent prendre les autorités de contrôle nationales et celui de rendre une décision contraignante dans certains cas de figure.

B. Avis du CEPD

1. Saisine obligatoire par une autorité de contrôle de données personnelles

Chaque fois qu'une autorité de contrôle compétente envisage d'adopter certaines mesures, elle va devoir saisir le CEPD afin que celui-ci émette un avis sur la mesure en question.

Les autorités de contrôle compétentes devront communiquer au CEPD chaque projet de décision qui concerne les points suivants :

1. lorsqu'elles entendent adopter une liste d'opérations de traitement pour lesquelles une analyse d'impact en matière de données personnelles (AIPD) doit être effectuée ;
2. lorsqu'elles doivent décider si un projet de code de conduite ou une modification ou une prorogation d'un code de conduite respecte le RGPD ;
3. lorsqu'elles vont approuver les critères d'agrément d'un organisme certificateur ;
4. lorsqu'elles entendent fixer des clauses contractuelles types de protection des données en matière de transfert ou lorsque ces clauses concernent la relation contractuelle entre un responsable et un sous-traitant ;
5. lorsqu'elles voudraient approuver des règles d'entreprises contraignantes (BCR).

L'autorité de contrôle compétente qui a saisi le CEPD n'adopte pas son projet de décision tant que le délai de réponse du CEPD court (voyez plus bas).

L'autorité de contrôle tient le plus grand compte de l'avis du CEPD et fait savoir au président du CEPD par voie électronique au moyen d'un formulaire type, dans un délai de deux semaines suivant la réception de l'avis, si elle maintiendra ou si elle modifiera son projet de décision et, le cas échéant, son projet de décision modifié.

Si l'autorité de contrôle de données personnelles entend ne pas suivre, totalement ou seulement en partie, l'avis du CEPD, elle doit en informer le président du CEPD dans ce délai de deux semaines. Cette communication doit être accompagnée des raisons qui sous-tendent le choix de l'autorité de contrôle de données personnelles.

Dans un tel cas de figure, le CEPD peut encore adopter une décision contraignante conformément à l'art. 65.1 du RGPD.

2. Saisine facultative

Toute autorité de contrôle, le président du CEPD ou la Commission européenne peuvent demander que toute question d'application générale ou produisant des effets dans plusieurs États membres de l'Union européenne soit examinée par le CEPD en vue d'obtenir un avis, en particulier lorsqu'une autorité de contrôle compétente ne respecte pas les obligations relatives à l'assistance mutuelle (art. 61 du RGPD) ou les obligations relatives aux opérations conjointes (art. 62 du RGPD).

3. Délai de réponse du CEPD et coopération des autorités de contrôle de données personnelles consultées par le CEPD

Le CEPD émettra un avis sur la question qui lui est soumise (soit en cas de saisine obligatoire, soit en cas de saisine facultative), à condition qu'il n'ait pas déjà émis un avis sur la même question.

Cet avis est adopté dans un délai de huit semaines à la majorité simple des membres du comité. Ce délai peut être prolongé de six semaines en fonction de la complexité de la question.

En ce qui concerne le projet de décision transmis au CEPD par une autorité de contrôle de données personnelles et par après transmis par le CEPD lui-même à ses membres, un membre qui n'a pas formulé d'objection dans un délai raisonnable fixé par le président est réputé approuver le projet de décision.

Les autorités de contrôle et la Commission européenne communiquent, dans les meilleurs délais, au CEPD, par voie électronique et au moyen d'un formulaire type, toutes les informations utiles, y compris, selon le cas, un résumé des faits, le projet de décision, les motifs rendant nécessaire l'adoption de cette mesure et les points de vue des autres autorités de contrôle concernées.

Le président du CEPD transmet dans les meilleurs délais par voie électronique :

1. toutes les informations utiles qui lui ont été communiquées à ses membres et à la Commission, au moyen d'un formulaire type. Le secrétariat du CEPD fournit, si nécessaire, les traductions des informations utiles et
2. l'avis à l'autorité de contrôle concernée et à la Commission européenne.

Le CEPD publiera sur son site web l'avis qu'elle a transmis à l'autorité de contrôle de données personnelles et à la Commission européenne (principe de transparence).

C. Règlement des litiges par le CEPD

1. Les décisions contraignantes du CEPD

En vue d'assurer l'application correcte et cohérente du RGPD, le CEPD peut adopter une décision contraignante dans certaines situations.

Ces situations sont les suivantes :

1. lorsque, en matière de coopération obligatoire entre les autorités de protection, une autorité de contrôle concernée a formulé une objection

pertinente et motivée à l'égard d'un projet de décision de l'autorité de contrôle chef de file ou que l'autorité de contrôle chef de file a rejeté cette objection au motif qu'elle n'est pas pertinente ou motivée. La décision contraignante concerne toutes les questions qui font l'objet de l'objection pertinente et motivée, notamment celle de savoir s'il y a violation ou non du RGPD ;

2. lorsqu'il existe des points de vue divergents quant à l'autorité de contrôle concernée qui est compétente pour l'établissement principal d'une société ;
3. lorsqu'une autorité de contrôle compétente ne demande pas l'avis du CEPD alors qu'elle le devrait (cas de la saisine obligatoire vu *supra*) ou qu'elle ne suit pas l'avis du CEPD émis que ce soit en cas de saisine obligatoire ou de saisine facultative. Dans ce cas, toute autorité de contrôle concernée ou la Commission européenne peut saisir le CEPD de la question.

2. Délais et majorités

La décision contraignante du CEPD est adoptée à la majorité des deux tiers des membres du comité dans un délai d'un mois à compter de la transmission de la question. Ce délai peut être prolongé d'un mois en fonction de la complexité de la question.

La décision contraignante est motivée et est adressée à l'autorité de contrôle chef de file et à toutes les autorités de contrôle concernées et est contraignante à leur égard.

Lorsque le CEPD n'a pas été en mesure d'adopter une décision dans les délais, il adopte sa décision, à la majorité simple de ses membres, dans un délai de deux semaines suivant l'expiration du deuxième mois. En cas d'égalité des voix au sein du comité, la voix de son président est prépondérante.

Les autorités de contrôle concernées n'adoptent pas de décision sur la question soumise au CEPD tant que les délais courent.

Le président du CEPD notifie, dans les meilleurs délais, la décision contraignante aux autorités de contrôle concernées. Il en informe aussi la Commission européenne. La décision est publiée sur le site internet du CEPD sans tarder après que l'autorité de contrôle a notifié sa décision finale au CEPD.

D. La décision finale de l'autorité de contrôle de données personnelles

L'autorité de contrôle chef de file ou, selon le cas, l'autorité de contrôle auprès de laquelle la réclamation a été introduite, adopte sa décision finale sur la base de la décision contraignante du CEPD, dans les meilleurs délais et au plus tard un mois après que le CEPD lui a notifié sa décision. L'autorité de contrôle chef de file ou, selon le cas, l'autorité de contrôle auprès de laquelle la réclamation a été introduite, informe le CEPD de la date à laquelle sa décision finale est notifiée, respectivement, au responsable du traitement ou au sous-traitant et à la personne concernée.

La décision finale des autorités de contrôle concernées est adoptée sous certaines conditions (art. 60.7, 60.8 et 60.9 du RGPD). La décision finale fait référence à la décision contraignante du CEPD et précise que celle-ci sera publiée sur le site internet du CEPD.

La décision contraignante du CEPD sera jointe à la décision finale.

E. Procédure d'urgence

Dans des circonstances exceptionnelles, lorsqu'une autorité de contrôle concernée considère qu'il est urgent d'intervenir pour protéger les droits et libertés des personnes concernées, elle peut adopter immédiatement des mesures provisoires visant à produire des effets juridiques sur son propre territoire et ayant une durée de validité qui n'excède pas trois mois. L'autorité de contrôle communique sans tarder ces mesures et les raisons de leur adoption aux autres autorités de contrôle concernées, au CEPD et à la Commission européenne.

Lorsqu'une autorité de contrôle a pris une mesure d'urgence et estime que des mesures définitives doivent être adoptées d'urgence, elle peut demander un avis d'urgence ou une décision contraignante d'urgence au comité, en motivant sa demande d'avis ou de décision.

Toute autorité de contrôle peut, en motivant sa demande, requérir au CEPD un avis d'urgence ou une décision contraignante d'urgence lorsqu'une autorité de contrôle compétente n'a pas pris de mesure appropriée dans une situation où il est urgent d'intervenir afin de protéger les droits et libertés des personnes concernées.

L'avis d'urgence ou la décision contraignante d'urgence est adopté dans un délai de deux semaines à la majorité simple des membres du CEPD.

F. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 27 : Les autorités de contrôle indépendantes*
- *Fiche de guidance n° 28 : L'identification de l'autorité de contrôle chef de file en cas de transferts transfrontaliers (le guichet unique ou le « one-stop-shop »)*
- *Fiche de guidance n° 29 : La bonne coopération entre les autorités de contrôle des données personnelles*
- *Fiche de guidance n° 31 : Le CEPD (le « Comité européen de la protection des données »)*

Fiche de guidance n° 31
Le CEPD (le « Comité européen de la protection des données »)

Articles 68 à 76 du RGPD

Considérants 72, 77, 105, 124, 136 & 140 du RGPD

Le Comité européen de la protection des données (le « CEPD ») remplacera le 25 mai 2018 le Groupe de Travail « Article 29 ». Il réunira l'ensemble des autorités de contrôle nationales.

Le CEPD sera habilité à émettre des avis ou des autorisations concernant diverses questions telles que les règles institutionnelles contraignantes, les critères de certification et les codes de conduite utilisés par les entreprises ; à adopter des décisions contraignantes afin d'assurer la cohérence entre les autorités de contrôle et à émettre des avis et des orientations sur des questions pertinentes concernant l'interprétation et l'application du RGPD, comme l'a fait le Groupe de Travail « Article 29 ».

Ses compétences sont nombreuses et son influence sera grandissante.

A. Composition du Comité européen de la protection des données (CEPD)

Le CEPD est institué en tant qu'organe de l'Union, possède la personnalité juridique et est représenté par son président.

Le CEPD se compose du chef d'une autorité de contrôle de chaque État membre et du Contrôleur européen de la protection des données (présidé pour l'instant par M. Butarelli) ou de leurs représentants respectifs.

Lorsque, dans un État membre, plusieurs autorités de contrôle sont chargées de surveiller l'application des dispositions du présent règlement, un

représentant commun est désigné conformément au droit de cet État membre (clairement, le règlement vise ici la situation de l'Allemagne).

La Commission européenne a le droit de participer aux activités et aux réunions du CEPD mais sans droit de vote. La Commission désigne un représentant. Le président du CEPD informe la Commission des activités du CEPD.

Dans les cas visés à l'article 65, le Contrôleur européen de la protection des données ne disposera de droits de vote qu'à l'égard des décisions concernant des principes et des règles applicables aux institutions, organes et organismes de l'Union qui correspondent, en substance, à ceux énoncés dans le RGPD.

B. Indépendance

Le CEPD exerce ses missions et ses pouvoirs en toute indépendance.

Sans préjudice des demandes de la Commission européenne visées à l'article 70.1.b et à l'article 70.2 du RGPD, le CEPD ne sollicite ni n'accepte d'instructions de quiconque dans l'exercice de ses missions et de ses pouvoirs.

C. Missions du comité

Le CEPD veille à l'application cohérente du RGPD.

À cet effet, le CEPD, de sa propre initiative ou, le cas échéant, à la demande de la Commission européenne, a notamment pour missions :

1. de surveiller et de garantir la bonne application du RGPD dans les cas prévus aux articles 64 et 65 du Règlement, sans préjudice des missions des autorités de contrôle nationales ;
2. de conseiller la Commission européenne en ce qui concerne :
   a) toute question relative à la protection des données à caractère personnel dans l'Union européenne, y compris sur tout projet de modification du RGPD ;
   b) les règles d'entreprise contraignantes (les fameuses « BCR »), sur la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent ;
3. d'examiner, de sa propre initiative, à la demande de l'un de ses membres ou à la demande de la Commission européenne, toute question portant sur l'application du RGPD, et de publier des lignes directrices, des recommandations et des bonnes pratiques afin de favoriser l'application cohérente du Règlement ;

4. de publier des lignes directrices, des recommandations et des bonnes pratiques relatives :
   a) aux procédures de suppression des liens vers des données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication accessibles au public, ainsi que le prévoit l'article 17.2 du RGPD ;
   b) aux critères et conditions applicables aux décisions fondées sur le profilage en vertu de l'article 22.2 du RGPD ;
   c) aux violations de données à caractère personnel, aux délais visés à l'article 33.1 et 33.2 du RGPD en cas de violation de données à caractère personnel et aux circonstances particulières dans lesquelles un responsable du traitement ou un sous-traitant est tenu de notifier la violation de données à caractère personnel ;
   d) aux circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques comme le prévoit l'article 34.1 du RGPD ;
   e) aux critères et exigences applicables aux transferts de données à caractère personnel fondés sur des règles d'entreprise contraignantes appliquées par les responsables du traitement et par les sous-traitants et aux autres exigences nécessaires pour assurer la protection des données à caractère personnel des personnes concernées visées à l'article 47 du RGPD ;
   f) aux critères et exigences applicables aux transferts de données à caractère personnel sur la base de l'article 49.1 du RGPD ;
   g) aux procédures communes à établir pour permettre aux personnes physiques les signalements de violations du RGPD en vertu de l'article 54.2 du Règlement ;
5. d'élaborer, à l'intention des autorités de contrôle, des lignes directrices concernant l'application des mesures visées à l'article 58.1 (les pouvoirs d'enquête des autorités de contrôle), 58.2 (les mesures correctrices que peuvent prendre les autorités de contrôle) et 58.3 (les pouvoirs d'autorisation et les pouvoirs consultatifs des autorités de contrôle), ainsi que la fixation des amendes administratives en vertu de l'article 83 du RGPD ;
6. de faire le bilan de l'application pratique des lignes directrices, recommandations et des bonnes pratiques qu'il a émis ;
7. d'encourager l'élaboration de codes de conduite et la mise en place de mécanismes de certification et de labels et de marques en matière de protection des données en vertu des articles 40 et 42 du RGPD ;
8. de procéder à l'agrément des organismes de certification et à l'examen périodique de cet agrément en vertu de l'article 43 du RGPD et de tenir un registre public des organismes agréés en vertu de l'article 43.6,

ainsi que des responsables du traitement ou des sous-traitants agréés établis dans des pays tiers en vertu de l'article 42.7 du Règlement ;

9. de définir les exigences visées à l'article 43.3 du RGPD aux fins de l'agrément des organismes de certification prévu à l'article 42 du même Règlement ;
10. de rendre à la Commission européenne un avis sur les exigences en matière de certification visées à l'article 43.8 du RGPD ;
11. de rendre à la Commission européenne un avis sur les icônes visées à l'article 12.7 du RGPD ;
12. de rendre à la Commission européenne un avis en ce qui concerne l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers ou une organisation internationale, y compris concernant l'évaluation visant à déterminer si un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou une organisation internationale n'assurent plus un niveau adéquat de protection. À cette fin, la Commission européenne fournit au CEPD tous les documents nécessaires, y compris la correspondance avec le gouvernement du pays tiers, en ce qui concerne ledit pays tiers, territoire ou secteur déterminé ou avec l'organisation internationale ;
13. d'émettre des avis sur les projets de décisions des autorités de contrôle conformément au mécanisme de contrôle de la cohérence visé à l'article 64.1, sur les questions soumises en vertu de l'article 64.2, et d'émettre des décisions contraignantes en vertu de l'article 65, y compris dans les cas visés à l'article 66 du RGPD ;
14. de promouvoir la coopération et l'échange bilatéral et multilatéral effectif d'informations et de bonnes pratiques entre les autorités de contrôle européennes ;
15. de promouvoir l'élaboration de programmes de formation conjoints et de faciliter les échanges de personnel entre autorités de contrôle, ainsi que, le cas échéant, avec les autorités de contrôle de pays tiers ou d'organisations internationales ;
16. de promouvoir l'échange, avec des autorités de contrôle de la protection des données de tous pays, de connaissances et de documentation sur la législation et les pratiques en matière de protection des données ;
17. d'émettre des avis sur les codes de conduite élaborés au niveau de l'Union européenne en application de l'article 40.9 du RGPD et
18. de tenir un registre électronique, accessible au public, des décisions prises par les autorités de contrôle et les juridictions sur les questions traitées dans le cadre du mécanisme de contrôle de la cohérence.

Lorsque la Commission européenne demande conseil au CEPD, elle peut mentionner un délai, selon l'urgence de la question.

Le CEPD transmet ses avis, lignes directrices, recommandations et bonnes pratiques à la Commission européenne et au comité de contrôle visé à l'article 93 du RGPD, et les publie.

Le CEPD consulte, le cas échéant, les parties intéressées et leur permet de formuler des observations dans un délai raisonnable. Il met les résultats de la procédure de consultation à la disposition du public, sans préjudice de l'article 76 du RGPD.

D. Rapports

Le CEPD établit un rapport annuel sur la protection des personnes physiques à l'égard du traitement dans l'Union européenne et, s'il y a lieu, dans les pays tiers et les organisations internationales. Le rapport est rendu public et communiqué au Parlement européen, au Conseil et à la Commission.

Le rapport annuel présente notamment le bilan de l'application pratique des lignes directrices, recommandations et bonnes pratiques visées à l'article 70.1.l ainsi que des décisions contraignantes visées à l'article 65 du RGPD.

E. Procédure

Le CEPD prend ses décisions à la majorité simple de ses membres, sauf disposition contraire du RGPD.

Le CEPD adopte son règlement intérieur à la majorité des deux tiers de ses membres et détermine ses modalités de fonctionnement.

F. Président

Le CEPD élit son président et deux vice-présidents en son sein à la majorité simple.

Le président et les vice-présidents sont élus pour un mandat de cinq ans renouvelable une fois.

G. Missions du président

Le président du CEPD a pour missions :

1. de convoquer les réunions du CEPD et d'établir l'ordre du jour ;
2. de notifier les décisions adoptées par le CEPD en application de l'article 65 à l'autorité de contrôle chef de file et aux autorités de contrôle concernées ;
3. de veiller à l'accomplissement, dans les délais, des missions du CEPD, notamment en ce qui concerne le mécanisme de contrôle de la cohérence visé à l'article 63.

Le CEPD fixe dans son règlement intérieur la répartition des tâches entre le président et les vice-présidents.

H. Secrétariat

Le CEPD dispose d'un secrétariat, qui est assuré par le Contrôleur européen de la protection des données.

Le secrétariat accomplit ses tâches sous l'autorité exclusive du président du CEPD.

Le personnel du Contrôleur européen de la protection des données qui participe à l'exercice des missions que le RGPD confie au CEPD est soumis à une structure hiérarchique distincte de celle du personnel qui participe à l'exercice des missions confiées au Contrôleur européen de la protection des données.

Le cas échéant, le CEPD et le Contrôleur européen de la protection des données établissent et publient un protocole d'accord fixant les modalités de leur coopération et s'appliquant au personnel du Contrôleur européen de la protection des données qui participe à l'exercice des missions que le RGPD confie au CEPD.

Le secrétariat fournit un soutien analytique, administratif et logistique au CEPD.

Le secrétariat est notamment chargé de :

1. la gestion courante du comité ;
2. la communication entre les membres du comité, son président et la Commission ;
3. la communication avec d'autres institutions et le public ;
4. l'utilisation des voies électroniques pour la communication interne et externe ;
5. la traduction des informations utiles ;

6. la préparation et le suivi des réunions du comité ;
7. la préparation, la rédaction et la publication d'avis, de décisions relatives au règlement des litiges entre autorités de contrôle et d'autres textes adoptés par le comité.

I. Confidentialité

Lorsque le CEPD le juge nécessaire, ses débats sont confidentiels, comme le prévoit son règlement intérieur.

J. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 27 : Les autorités de contrôle indépendantes*
- *Fiche de guidance n° 28 : L'identification de l'autorité de contrôle chef de file en cas de transferts transfrontaliers (le guichet unique ou le « one-stop-shop »)*
- *Fiche de guidance n° 29 : La bonne coopération entre les autorités de contrôle des données personnelles*
- *Fiche de guidance n° 30 : Le mécanisme de contrôle de la cohérence*

Fiche de guidance n° 32
Les voies de recours et les responsabilités

Articles 77 à 82 du RGPD

Considérants 7, 141 à 145, 147 du RGPD

A. Le sous-traitant pleinement concerné par les nouvelles règles

Actuellement, seule la responsabilité des responsables du traitement peut être mise en cause. Après le 25 mai 2018, la non-conformité tant des sous-traitants que des responsables du traitement pourra être sanctionnée !

Le RGPD permet aux consommateurs d'obtenir plus facilement compensation dans le cas où ils ont subi un dommage matériel ou non matériel du fait d'un traitement non conforme aux règles du RGPD.

Lorsque tant le responsable du traitement que le sous-traitant sont concernés, chacune des parties pourra être requise de compenser l'entièreté du dommage subi.

Voyons ci-dessous plus en détail les règles du RGPD en matière de responsabilité. Nous vous expliquerons tout d'abord devant quelle autorité la personne concernée peut intenter une action (point B). Nous verrons ensuite qui sera responsable, selon les nouvelles règles, de compenser le dommage subi par la personne concernée (point C).

B. Voies de recours et responsabilité

1. Droit d'introduire une réclamation auprès d'une autorité de contrôle par une personne concernée

Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du RGPD.

Quelle autorité de contrôle saisir ?

La personne concernée a le choix.

Elle peut saisir :

1. l'autorités de protection de données personnelles dans lequel se trouve sa résidence habituelle ;
2. l'autorité de contrôle de données personnelles de son lieu de travail ;
3. l'autorité de contrôle de données personnelles où la violation aurait été commise.

L'autorité de contrôle auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel.

2. Droit à un recours juridictionnel effectif contre une autorité de contrôle de toute personne physique ou morale

Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne physique ou morale a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne.

Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne concernée a le droit de former un recours juridictionnel effectif lorsque l'autorité de contrôle qui est compétente en vertu des articles 55 et 56 du RGPD ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite au titre de l'article 77 du RGPD.

Toute action contre une autorité de contrôle est intentée devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie.

Dans le cas d'une action intentée contre une décision d'une autorité de contrôle qui a été précédée d'un avis ou d'une décision du CEPD dans le cadre du mécanisme de contrôle de la cohérence, l'autorité de contrôle transmet l'avis ou la décision en question à la juridiction concernée.

3. Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant par une personne concernée

Sans préjudice de tout recours administratif ou extrajudiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77 du RGPD, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le RGPD ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du RGPD.

Quelle juridiction saisir ?

1. Toute action contre un responsable du traitement ou un sous-traitant est intentée devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement.
2. Une telle action peut aussi être intentée devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle,
   - sauf si le responsable du traitement ou le sous-traitant est une autorité publique d'un État membre agissant dans l'exercice de ses prérogatives de puissance publique.

4. Représentation des personnes concernées

La personne concernée a le droit de mandater un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel les concernant, pour qu'il introduise une réclamation en son nom, exerce en son nom les droits visés aux articles 77, 78 et 79 du RGPD et exerce en son nom le droit d'obtenir réparation visé à l'article 82 lorsque le droit d'un État membre le prévoit.

Les États membres peuvent prévoir que tout organisme, organisation ou association en question, indépendamment de tout mandat confié par une personne concernée, a, dans l'État membre en question, le droit d'introduire une réclamation auprès de l'autorité de contrôle qui est compétente en vertu de l'article 77 du RGPD et d'exercer les droits visés aux articles 78 et 79 s'il considère

que les droits d'une personne concernée prévus au RGPD ont été violés du fait du traitement.

Les États membres sont donc libres de permettre la création de cette nouvelle sorte d'action de groupe (ou « class action ») en matière de protection des données personnelles. Nous espérons que beaucoup d'États activeront cette possibilité ouverte par le RGPD et que beaucoup d'associations se créeront en la matière. En effet, souvent ce sont des actions de groupe ou collective qui ont permis l'établissement de véritables normes protectrices des droits des citoyens.

Nous en ferons le bilan dans quelques années.

5. Suspension d'une action

Lorsqu'une juridiction compétente d'un État membre est informée qu'une action concernant le même objet a été intentée à l'égard d'un traitement effectué par le même responsable du traitement ou le même sous-traitant et est pendante devant une juridiction d'un autre État membre, elle contacte cette juridiction dans l'autre État membre pour confirmer l'existence d'une telle action (litispendance).

Lorsqu'une action concernant le même objet a été intentée à l'égard d'un traitement effectué par le même responsable du traitement ou le même sous-traitant et est pendante devant une juridiction d'un autre État membre, toute juridiction compétente autre que la juridiction saisie en premier lieu peut suspendre son action.

Lorsque cette action est pendante devant des juridictions du premier degré, toute juridiction autre que la juridiction saisie en premier lieu peut également se dessaisir, à la demande de l'une des parties, à condition que la juridiction saisie en premier lieu soit compétente pour connaître des actions en question et que le droit applicable permette leur jonction.

C. Droit à réparation et responsabilité

Nous connaissons maintenant la règle générale : toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du RGPD.

Un sous-traitant ne sera tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le RGPD qui

incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

Un responsable du traitement ou un sous-traitant est exonéré de responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.

Cette exemption de responsabilité semble être devoir interprétée plus restrictivement que celle qui existe à l'article 23.2 de la Directive de 1995 : « Le responsable du traitement peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable. ».

Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsqu'ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.

Toutefois, lorsqu'un responsable du traitement ou un sous-traitant a réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage.

Par exemple, un sous-traitant pourrait être tenu de payer à la personne concernée 100 % de son dommage même s'il n'est responsable que de 1 % du dommage subi par ladite personne concernée. À charge par après pour le sous-traitant de se retourner contre le responsable du traitement pour se faire rembourser les sommes qui ne correspondent pas à sa responsabilité.

D. Difficultés

On vient de le lire, les règles en la matière sont assez complexes et certainement être source de futures discussions. Elles mélangent en effet les règles en matière de responsabilité vis-à-vis de la personne concernée et celles de partage entre responsables du dommage indemnisé.

Surtout que, pour les éclairer, pour une fois, le Règlement ne contient qu'un seul considérant que nous reproduisons ici. Il s'agit du considérant 146 :

> « Le responsable du traitement ou le sous-traitant devrait réparer tout dommage qu'une personne peut subir du fait d'un traitement effectué en violation du présent règlement.
>
> Le responsable du traitement ou le sous-traitant devrait être exonéré de sa responsabilité s'il prouve que le dommage ne lui est nullement imputable.

> La notion de dommage devrait être interprétée au sens large, à la lumière de la jurisprudence de la Cour de justice, d'une manière qui tienne pleinement compte des objectifs du présent règlement.
>
> Cela est sans préjudice de toute action en dommages-intérêts fondée sur une infraction à d'autres règles du droit de l'Union ou du droit d'un État membre. Un traitement effectué en violation du présent règlement comprend aussi un traitement effectué en violation des actes délégués et d'exécution adoptés conformément au présent règlement et au droit d'un État membre précisant les règles du présent règlement.
>
> Les personnes concernées devraient recevoir une réparation complète et effective pour le dommage subi.
>
> Lorsque des responsables du traitement ou des sous-traitants participent à un même traitement, chaque responsable du traitement ou chaque sous-traitant devrait être tenu responsable pour la totalité du dommage.
>
> Toutefois, lorsque des responsables du traitement et des sous-traitants sont concernés par la même procédure judiciaire, conformément au droit d'un État membre, la réparation peut être répartie en fonction de la part de responsabilité de chaque responsable du traitement ou de chaque sous-traitant dans le dommage causé par le traitement, à condition que le dommage subi par la personne concernée soit entièrement et effectivement réparé.
>
> Tout responsable du traitement ou tout sous-traitant qui a réparé totalement le dommage peut par la suite introduire un recours contre d'autres responsables du traitement ou sous-traitants ayant participé au même traitement ».

De plus, le RGPD est muet sur des notions centrales comme la détermination du dommage subi en cas de perte de données personnelles (même si le considérant 146 précise que la notion de dommage doit être interprétée largement). Comment en effet déterminer financièrement un dommage subi dans l'ensemble des hypothèses visées par les considérants 75 et 85 du RGPD ? En cas de traitement non conforme au RGPD ? Lorsque la personne concernée n'a pas été correctement informée ? Lorsque le responsable du traitement n'a pas répondu dans le délai d'un mois ? Surtout que souvent, la personne concernée risque de subir un dommage moral et un dommage réputationnel (si ce n'est la même chose).

Les spécialistes se tourneront adéquatement vers les règles existantes et complexes du droit de la preuve.

Cette incertitude est préjudiciable tant pour les personnes concernées que les entreprises qui ne sauront pas quelle somme provisionner pour pallier d'éventuels litiges en cas, par exemple, d'attaques informatiques ayant fait subir un préjudice à des personnes concernées.

Fiche de guidance n° 33
Les sanctions et leur caractère dissuasif

Articles 83 et 84 du RGPD

Considérants 148 à 151 du RGPD

A. Introduction

Dans le cas où il se trouverait qu'une société n'est pas en conformité avec les (nombreuses) exigences du RGPD, les conséquences financières pourraient être très élevées. Et n'oublions pas, à l'heure d'internet, les possibles répercussions sur sa réputation.

B. Conditions générales pour imposer des amendes administratives

Chaque autorité de contrôle nationale devra veiller à ce que les amendes administratives imposées en violations du RGPD soient, dans chaque cas, effectives, proportionnées et dissuasives.

Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées par les autorités de contrôle en complément ou à la place des mesures correctrices visées à l'article 58.2.a à 58.2.h et 58.2.j du RGPD.

Le Groupe de Travail « Article 29 » recommande la création d'un groupe de travail au sein du futur comité européen de la protection des données (CEDP) consacré à l'échange d'informations entre les autorités de contrôle nationales sur leur pratique (lignes directrices, jurisprudence, avis) en la matière. Cet échange d'informations devrait favoriser (grâce, pourquoi pas, à des workshops réguliers) une interprétation et application cohérente et uniforme du RGPD à

travers toute l'Union européenne. Il serait en effet mal venu que les autorités de contrôle (même si elles sont indépendantes l'une de l'autre) prennent des mesures totalement différentes dans des cas similaires alors que les règles sont dorénavant codifiées dans un Règlement européen.

Pour décider s'il y a lieu d'imposer une amende administrative et pour décider de son montant, l'autorité de contrôle nationale devra tenir compte, après avoir dûment analysé chaque cas d'espèce, des éléments suivants (article 82.2 du RGPD) :

1. de la nature, gravité et durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi.

   Le nombre de personnes concernées affectées devrait être identifié dans le but de savoir s'il s'agit d'un événement isolé ou correspondant à une violation plus généralisée tandis que la durée de la violation pourrait être la démonstration que le responsable du traitement n'a pas pris les mesures de sécurité adéquates autour des données personnelles ;

2. du fait que la violation a été commise délibérément (par exemple, des traitements illicites exigés par la direction de la société et ce malgré un avis défavorable du DPD de la société en question) ou par négligence (à cause, par exemple d'une erreur humaine).

   Rappelons qu'il est de la responsabilité du responsable du traitement/sous-traitant de mettre en place les contrôles et les mesures adéquates en fonction de la complexité de leurs activités. Dès lors, ils ne peuvent déclarer par après ne pas être responsables de manquements juste en déclarant qu'ils n'ont pas eu les moyens financiers de mettre en place ces mesures de protection ;

3. de toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ou pour empêcher qu'il ne s'aggrave.

   Une telle attitude démontrera en effet que la société se sent responsable de ses activités de traitement ;

4. du degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 (« Protection des données dès la conception et protection des données par défaut ») et 32 (« Sécurité du traitement ») du RGPD. Il s'agit ici pour l'autorité de contrôle d'analyser en profondeur la manière dont le responsable du traitement a organisé la protection autour des données à caractère personnel collectées afin de répondre à cette simple question : compte tenu de la nature, des finalités et des tailles de ses traitements, le responsable du traitement a-t-il fait tout ce qu'il pouvait pour empêcher

le manquement constaté au vu des obligations qui s'imposent à lui en vertu du RGPD ?

5. de toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant, que ce soit la même violation qui vient à se répéter voire d'autres qui démontreraient alors des manquements d'organisation plus sérieux ;
6. du degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer de manière significative ou pas les éventuels effets négatifs ;
7. des catégories de données à caractère personnel concernées par la violation (s'agit de données sensibles ou pas ? Les données sont-elles cryptées ? etc.) ;
8. de la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation. Il sera tenu compte par l'autorité de contrôle du fait que la notification a été réalisée dans les délais requis et d'une manière complète ;
9. du fait de savoir si des mesures visées à l'article 58.2 du RGPD, ont été ou non précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet et du respect ou non de ces mesures ;
10. de l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 du RGPD. Un code de conduite comprendra (au futur car il n'en existe pas encore) les mécanismes qui devront veiller à son bon respect par les responsables du traitement ou les sous-traitants qui s'engagent à l'appliquer (sans préjudice bien sûr des missions et des pouvoirs des autorités de contrôle).

    En cas de manquement constaté et « sanctionné » par le mécanisme de contrôle d'un code de conduite que le responsable s'était engagé à respecter, il pourrait arriver que l'autorité de contrôle compétente s'en satisfasse. L'autorité de contrôle compétente pourrait considérer que, dans le cas d'espèce, les mesures prises par l'organisme chargé de veiller au contrôle du code de conduite en question a pris une mesure suffisamment effective, proportionnée et dissuasive que pour ne pas avoir à prendre elle une mesure supplémentaire. L'organisme chargé du respect du code de conduite peut aller jusqu'à suspendre ou exclure le responsable du traitement ou le sous-traitant concerné de l'application du code de conduite en question ;
11. de toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

Si un responsable du traitement ou un sous-traitant viole délibérément ou par négligence plusieurs dispositions du RGPD, dans le cadre de la même

opération de traitement ou d'opérations de traitement liées, le montant total de l'amende administrative ne pourra pas excéder le montant fixé pour la violation la plus grave. Dès lors, si des violations à l'article 8 et à l'article 12 du RGPD ont été découvertes, l'autorité de contrôle devra appliquer les mesures correctrices mentionnées à l'article 83.5 du RGPD qui correspond au montant fixé pour la violation la plus grave, autrement dit celle relative à l'article 12.

Après avoir analysé le cas qui lui est soumis et après avoir tenu compte des éléments mentionnés *supra*, l'autorité de contrôle prendra la mesure correctrice la plus appropriée. L'autorité de contrôle peut bien sûr prendre plusieurs mesures correctrices. Lorsque le manquement concerne l'un des cas mentionnés aux paragraphes 4 à 6 de l'article 83 du RGPD, l'autorité de contrôle devra inclure une possible amende (seule ou accompagnée d'une ou plusieurs autre(s) mesure(s) correctrice(s)) dans sa réflexion.

Le but, ne l'oublions pas, des mesures correctrices prises par l'autorité de contrôle est de restaurer la conformité à la Loi du traitement.

Le Groupe de Travail « Article 29 » rappelle que les amendes sont une mesure correctrice importante que les autorités de contrôle ne devraient activer que si cela est nécessaire. Une analyse fine de chaque cas sera à réaliser afin de déterminer si une amende administrative est la mesure correctrice la plus adéquate.

Le RGPD prévoit des amendes légères et des amendes lourdes pour les manquements qu'il considère comme les plus sévères. Les États membres peuvent étendre la liste des dispositions mentionnées aux paragraphes 4 à 6 de l'article 83 du RGPD.

Selon le considérant 148, « en cas de violation mineure ou si l'amende susceptible d'être imposée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende ». Ce n'est pas une obligation pour l'autorité de contrôle, juste une possibilité. Lorsque l'autorité de contrôle, au vu du cas soumis, entend imposer une amende administrative à une personne physique, l'autorité de contrôle doit analyser si l'amende ne constitue pas une charge disproportionnée et s'il ne serait pas plus appropriée d'adresser à la personne physique un simple rappel à l'ordre.

Amendes « légères »

Les violations des points suivants font l'objet d'amendes administratives pouvant s'élever jusqu'à 10.000.000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :

1. les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 8, 11, 25 à 39, 42 et 43 du RGPD ;
2. les obligations incombant à l'organisme de certification en vertu des articles 42 et 43 du RGPD ;
3. les obligations incombant à l'organisme chargé du suivi des codes de conduite en vertu de l'article 41.4 du RGPD.

Amendes « sévères »

Les violations des dispositions suivantes font l'objet d'amendes administratives pouvant s'élever jusqu'à 20.000.000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :

1. les principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 5, 6, 7 et 9 du RGPD ;
2. les droits dont bénéficient les personnes concernées en vertu des articles 12 à 22 du RGPD ;
3. les transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale en vertu des articles 44 à 49 du RGPD ;
4. toutes les obligations découlant du droit des États membres adoptées en vertu du chapitre IX du RGPD ;
5. le non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par l'autorité de contrôle en vertu de l'article 58.2, ou le fait de ne pas accorder l'accès prévu, en violation de l'article 58.1 du RGPD.

Le non-respect d'une mesure correctrice émise par l'autorité de contrôle en vertu de l'article 58.2, fait l'objet d'amendes administratives pouvant s'élever jusqu'à 20.000.000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Ce n'est pas parce qu'un manquement semble devoir être soumis à une amende légère que ce sera automatiquement le cas. En effet, dans certaines circonstances comme par exemple si le manquement a déjà fait l'objet d'un rappel à l'ordre de la part de l'autorité de contrôle compétente, rappel à l'ordre que le responsable du traitement n'a pas suivi, le manquement pourrait être soumis à l'amende la plus sévère.

Il n'est donc pas question d'automatisme mais de véritable analyse cas d'espèce après cas d'espèce.

Sans préjudice des pouvoirs dont les autorités de contrôle disposent en matière d'adoption de mesures correctrices en vertu de l'article 58.2 du RGPD, chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire.

L'exercice, par l'autorité de contrôle, de ses pouvoirs est soumis à des garanties procédurales appropriées conformément au droit de l'Union européenne et au droit des États membres, y compris un recours juridictionnel effectif et une procédure régulière.

Si le système juridique d'un État membre ne prévoit pas d'amendes administratives, l'amende est déterminée par l'autorité de contrôle compétente et imposée par les juridictions nationales compétentes, tout en veillant à ce que

les voies de droit soit effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle.

En tout état de cause, principe de base, les amendes imposées sont effectives, proportionnées et dissuasives. Elles doivent adéquatement répondre à la nature, à la gravité et aux conséquences du manquement que ce manquement concerne un traitement local ou transfrontière.

C. Autres sanctions

Les États membres détermineront le régime des autres sanctions applicables en cas de violations du RGPD, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83 du RGPD, et prendront toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont également effectives, proportionnées et dissuasives.

Chaque État membre notifiera à la Commission européenne les dispositions légales qu'il a adopté à ce sujet au plus tard le 25 mai 2018 et, sans tarder, toute modification ultérieure les concernant.

D. Ligne directrices du Groupe de Travail « Article 29 »

Le Groupe de Travail a publié le 4 octobre 2017 des Lignes directrices sur l'application et l'imposition des amendes dans le cadre du RGPD (Réf. WP 253).

E. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

➠ *la Fiche de guidance n° 27 : Les autorités de contrôle indépendantes*

Fiche de guidance n° 34
L'approche basée sur les risques dans le RGPD

A. Principe

Le principe d'*accountability* exige que les sociétés implémentent des mesures de sécurité autour des données qu'elles stockent. Ces mesures vont devoir être appropriées et dépendre dans chaque cas de la nature, de la portée, du contexte et des finalités du traitement. Elles vont aussi dépendre des risques des traitements par rapport aux droits et libertés des personnes concernées.

La société doit donc développer des contrôles appropriés qui sont en rapport avec le degré des risques associés à ses propres activités de traitement. Les mesures seront donc différentes de société en société en fonction des risques commerciaux que chaque société en tant qu'entrepreneur est prête à prendre et à assumer.

C'est ce que l'on appelle le « *Risk Based Approach* ».

Au plus les risques du traitement envisagé vis-à-vis des personnes concernées sont sévères et sérieux, au plus la société va devoir implémenter des mesures pour diminuer ces risques. Le RGPD exige que les entreprises évaluent les risques liés aux données personnelles qu'elles ont collectées (et qu'elles stockent toujours temporairement !) en prenant en considération la situation des personnes concernées. La question que les sociétés doivent se poser est celle-ci : quelles peuvent être les conséquences, en cas de violation(s) de données, vis-à-vis non pas de moi société mais vis-à-vis des personnes concernées qui restent toujours propriétaires de leurs données ?

Les personnes concernées n'ont en quelque sorte que prêté leurs données personnelles aux responsables du traitement le temps des traitements. Jamais indéfiniment, jamais pour n'importe quel traitement, jamais sans information. Et surtout en ayant confiance dans la sécurité du responsable du traitement.

Le risque doit faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données ne comportent aucun risque (rare), comportent un risque, un risque élevé voire très élevé.

B. Conséquences

C'est pourquoi, lorsque c'est nécessaire et approprié, une société devra réaliser une analyse d'impact relative à la protection des données (une AIPD) qui se focalisera sur les droits et libertés des personnes concernées. L'AIPD sera à réévaluer régulièrement.

Les mesures de protection des données devront être conçues dès la première étape de développement du produit ou du service. C'est ce que l'on appelle la *Privacy by Design*.

Les entreprises devront aussi continuellement mettre à jour les données stockées, leur infrastructure informatique (si nécessaire l'adapter et la renforcer), l'information qu'elles fournissent aux personnes concernées, les moyens qu'elles mettent à leur disposition afin de permettre leur d'exercer leurs droits, leurs procédures internes afin de toujours être capable de répondre à temps et adéquatement aux demandes des personnes concernées et/ou des autorités de protection, etc.

Les entreprises doivent continuellement se remettre en question et concevoir des produits et services toujours en adéquation avec le RGPD.

C'est un vrai challenge et une remise en question continuelle.

Fiche de guidance n° 35
Le big data et le RGPD

A. Introduction

Data, *Big Data*, *Open Data*, *Artificial Intelligence*, recrutement prédictif, justice prédictive, *political microtargeting*, etc. ces concepts, parfois détournés en *buzzwords*, sont aujourd'hui au cœur de toutes les stratégies marketing et commerciales des sociétés actuelles. Les sociétés se disent qu'il est indispensable, pour leur croissance, de réaliser des croisements de données, d'effectuer du big data et de l'analyse de mégadonnées.

Les données sont une « nouvelle » ressource et un véritable levier de compétitivité pour les entreprises. Bien souvent, les masses de données possédées par une société regroupent beaucoup de données personnelles en particulier. Réaliser de l'analyse de big data permettrait à une société d'améliorer sa performance opérationnelle/industrielle, sa performance commerciale et de mieux connaître ses clients. Certaines sociétés sont aussi tentées de vendre cette connaissance, parfois avec l'accord (implicite souvent) des clients, parfois aussi sans.

L'intérêt du *profiling* est grandissant et multiple.

En s'appuyant sur des algorithmes, sur le *machine learning* et la *data science*, l'analyse prédictive permet d'exploiter tout type de données pour mettre en place de nouveaux modèles d'interprétation et de prédiction, en tirer des prévisions sur des évolutions futures et émettre des recommandations sur les actions à mener.

Citons les exemples les plus répandus :

- la maintenance prédictive : analyser les signaux de la chaîne de production pour anticiper des défaillances et changer les pièces avant que la panne ne se produise ;
- la détection des fraudes : détecter des fraudes ou des pannes pour agir avant qu'elles ne se produisent ;

- l'analyse des comportements des clients : comprendre leurs motivations, identifier les meilleures façons de les prospecter et de les fidéliser pour proposer à chacun des services personnalisés au bon moment par le canal le plus pertinent ;
- l'influence politique sur les réseaux sociaux grâce à la publication sur ceux-ci de messages ciblés en fonction du propriétaire du compte du réseau.

L'idée principale derrière est, en matière de marketing, d'envoyer de meilleures campagnes de marketing direct électronique, des campagnes plus ciblées et donc plus efficaces (se disent du moins tous les responsables des services « marketing » ou de « *customer & data* »).

Imaginons par exemple une enseigne active dans la grande distribution. Celle-ci enregistre annuellement des millions de données concernant ses clients. En effet, lors du passage à la caisse et grâce à la lecture de sa carte de fidélité, l'enseigne collecte les données relatives aux achats. Si l'enseigne permet aussi l'achat en ligne (via un ou plusieurs sites différents mais gérés centralement), elle va aussi enregistrer des données relatives à ces achats via le web.

La société pourrait décider de croiser ces données, de les rassembler en les liant à un identifiant abstrait (donc de rendre les données anonymes) afin de pouvoir améliorer la connaissance de ses segments d'achats. Autrement dit, afin d'améliorer le profilage qu'elle réalise probablement déjà de ses clients dans son service marketing.

Notons que rien n'empêche l'enseigne de vendre à travers des grandes plateformes d'achat d'inventaires publicitaires qui existent déjà les données de ses clients qu'elle a anonymisées.

B. Qu'est-ce que le big data ?

1. Les quatre V

Pour expliquer le phénomène du big data, il est d'usage de faire référence aux trois V :

1. le Volume massif de données ;
2. la Variété des données ;
3. la Vitesse à laquelle il est dorénavant possible de collecter et de traiter les données (en temps réel même parfois).

On y ajoute aussi un V relatif à la Valeur des données collectées, traitées et interprétées. Au plus les données ont de la valeur, au plus le résultat sera intéressant pour l'entreprise.

Le big data s'entend donc comme des données informatives de gros volumes, d'une vélocité élevée et d'une grande variété qui nécessitent de nouvelles formes de traitement pour permettre une meilleure prise de décision.

L'intérêt du traitement des données massives est de découvrir de nouvelles corrélations pour de nouveaux usages qui sont généralement sans rapport avec les finalités originales pour lesquelles les données ont été collectées.

2. Le data storytelling

Ces nouvelles corrélations peuvent être découvertes grâce au data storytelling. Derrière le data storytelling, se cache une démarche consistant à explorer les données collectées par les systèmes d'information de la société et à les traduire en récit ou en langage courant. Le data storytelling consiste donc à faire parler les montagnes de données collectées par les systèmes d'information d'une entreprise et à découvrir des régularités, des relations, des spécificités qui permettent d'améliorer la performance de l'entreprise dans sa relation à ses clients, dans la course avec ses concurrents ou dans la conduite de ses opérations.

Derrière l'expression « big data » (ou données massives) se trouvent deux réalités.

L'opportunité, via la digitalisation massive des points de contact et la généralisation d'usage de capteurs dans les objets connectés (IoT), de connaître le détail de la vie de ses produits et des préférences de ses clients (et ce en temps réel ou presque). Il s'agit d'une opportunité pour les entreprises de développer leurs ventes, de fidéliser, d'améliorer la qualité de leurs produits/services et donc à terme de se transformer.

Le big data désigne aussi, et même avant tout, l'exploitation et l'interprétation des données générées par ces points de contact et des données fournies directement par les utilisateurs au travers des réseaux sociaux, les sites de vente, l'historique des recherches sur Google, des données publiques (open data), etc. pour des utilisations différentes. Toutefois, il faudra être prudent et faire en sorte que l'entreprise réussisse à filtrer à ses différents niveaux les informations inutiles et ne laisse passer que celles qui sont réellement pertinentes et de très bonne qualité. Il faut éviter ce que l'on appelle l'infobésité.

Pour pouvoir exploiter ces innombrables informations, d'importantes capacités de calcul sont nécessaires, souvent uniquement disponibles dans de grands data centers. De tels services sont mis à disposition par les pratiques d'externalisation informatique. Le *cloud computing* permet de louer (à des prix de moins en moins élevés) à distance une puissance de calcul et un espace de stockage adaptés à des traitements big data. Les ordinateurs de plus en plus puissants aidés par l'intelligence artificielle et le *machine learning* tenteront de percer à jour de plus en plus rapidement les clients et de les classer dans des segments ou profils préétablis souvent sans même qu'ils s'en rendent compte (et donc sans qu'ils aient pu accepter ce traitement).

Cette détermination en se basant sur des calculs issus de la probabilité n'est pas certaine à 100 % et donc n'est pas sans risque d'erreur. Il y aura

apparition de faux positifs et de faux négatifs. De plus, elle risque de perpétuer des erreurs et des discriminations issues du passé à cause de mauvaises données de départ et d'interprétations erronées lors de l'encodage des données.

3. Des utilisations multiples

Avec une utilisation adéquate des mégadonnées, le marché pourra améliorer l'intelligence économique et l'efficacité des secteurs privé et public, développer de nouvelles applications qui permettront à terme une exploitation de nouvelles opportunités sociales et économiques qui transformeront fondamentalement la société tout entière.

Les enseignements et les prédictions tirés du big data seront utiles aux entreprises et à tous leurs services.

Pour le service production pour leur permettre de créer au plus vite des produits adaptés aux besoins actuels des consommateurs et au service marketing pour mieux envoyer anticipativement des publicités ciblées aux prospects et aux clients. Le big data est aussi utile lors de la conclusion de contrats en ligne afin de connaître le futur client (lors d'un éventuel « *scoring* » de ce client) et ce même à son insu grâce à la collecte des données issues de ses objets connectées par exemple.

Ce seront les *data scientists*, spécialistes de la science des données qui devront, face à la multitude d'informations du big data, donner du sens et de la valeur à ces données, chercher des corrélations entre elles, repérer les anomalies… Ils vont concevoir des méthodes, des modèles et algorithmes pour collecter, stocker, traiter et restituer les données. Et ce dans le but d'aider l'entreprise à prendre des décisions stratégiques ou opérationnelles, que ce soit sur des thématiques liées au marketing, aux services, aux tendances d'achat ou de consommation, pour élaborer le profil de la clientèle dans le but de leur appliquer des décisions automatisées adéquates, déterminer ses attentes, …

C. Les questions soulevées par le RGPD

1. Présentation du sujet

Les questions soulevées par le big data sont pléthoriques :

- quelles données peut-on et doit-on conserver ?
- à qui appartiennent les données ainsi collectées, conservées, transférées, modifiées ou interprétées et qui en est responsable ?
- d'où proviennent les données objet des analyses ?

- où sont-elles stockées ?
- peut-on en faire ce que l'on veut ?
- que peut-on faire du résultat de la comparaison de celles-ci ?
- les données résultant de cette comparaison appartiennent-elles à celui qui a réalisé la comparaison ?
- sont-elles susceptibles de faire l'objet d'un commerce ?
- si oui, quels sont les règles juridiques qui régissent la commercialisation de ces données ?
- quelle est la sécurité qui entoure ces données ?
- qui y a accès ?
- faut-il avoir le consentement de la personne concernée pour réaliser ces opérations ?
- doit-on permettre un jour à des tiers américains d'y accéder via le *Patriot Act* par exemple ?
- quelle est la durée de conservation de chacune des catégories de données sachant que la durée légale de conservation varie de catégorie de données en catégorie de données ?

Le statut de chaque donnée dépend très largement de la nature des données concernées : données publiques ou privées, à caractère personnel ou non.

Il est donc primordial, avant de réaliser une opération sur une donnée, de s'interroger sur la famille à laquelle elle peut être rattachée puisque c'est cette famille qui va, dans une large mesure, déterminer les règles juridiques qui lui seront applicables. Il faut éviter de considérer que le gig data ne mène à des big problèmes !

Les *data analysts* vont avoir besoin d'outils informatiques performants afin de savoir très vite quel est le statut des données qu'ils vont analyser, leur provenance, etc.

Confondre archivage et sauvegarde pourrait aussi être une erreur fatale. L'archivage consiste à classer des originaux afin qu'ils puissent être ressortis à toute fin utile. De son côté, la sauvegarde se résume à copier les fichiers en vue de les restaurer si le besoin s'en fait sentir.

L'archivage se distingue aussi du stockage par la notion de sécurité qui les différencie. Contrairement aux documents stockés, ceux qui sont archivés ne peuvent être modifiés, leur destruction est impossible à moins d'un contrôle minutieux, et toute opération effectuée doit être répertoriée en vue d'être retracée.

Des archives questionnées efficacement sont bien plus qu'un gain de temps, elles sont génératrices de revenus. Or, le big data pousse les sociétés à tout archiver plutôt qu'à trier l'information pertinente et la séparer de celle qui est moins utile.

Le risque pour les entreprises est de se retrouver face à un flot de données inextricable. Avec pour conséquence un ralentissement dans certaines prises de décision et le développement de l'activité.

Bien conservées et exploitées, ces données constituent pourtant une mine de richesse.

En matière de big data, comme pour tout traitement de données à caractère personnel, chacun des principes du RGPD est important et devra être scrupuleusement respecté par le responsable du traitement.

Parcourons ici les points les plus importants.

Notons déjà une conclusion erronée : le big data et le RGPD ne font pas bon ménage. Les responsables du traitement devront analyser chacun de leur traitement qui implique et des données à caractère personnel (rappelons que les données anonymisées sont hors champ d'application du RGPD mais pas les données pseudonymisées qui sont des données personnelles) et des données massives.

2. Les difficultés liées à la protection des données personnelles

Souvent, la société voudra combiner dans son traitement big data des données qu'elles possèdent avec des données collectées par un tiers pour ses propres traitements. La société voudra traiter ces données dans un but différent de ce pour quoi les données ont été initialement collectées. La société pourrait réaliser un traitement mélangeant des données particulières au sens de l'article 9 du RGPD avec des données qui n'en sont pas.

Le responsable du traitement devra adéquatement s'interroger sur la base juridique qui sous-entendait la collecte de chacune des catégories de données afin de voir si le traitement ultérieur de big data est compatible avec le traitement initial.

Les réponses aux questions relatives au big data ne sont pas si évidentes. Tentons de dissiper quelque peu le brouillard.

Les principes de tout traitement se trouvent énoncés à l'article 5 du RGPD. Les bases juridiques des traitements sont énoncées à l'article 6 du même Règlement.

L'article 5, fondamental, énonce que tout traitement doit respecter les principes de licéité, de loyauté et de transparence, de limitation des finalités, de minimisation des données, d'exactitude, de limitation de conservation, d'intégrité et de confidentialité. Il reprend aussi le principe faîtier d'*accountability*.

a. *Le principe de limitation des finalités (ancien principe de proportionnalité)*

Ainsi, le principe de limitation des finalités rappelle que les données doivent être collectées pour des finalités déterminées, explicites et légitimes. Les données ne pourront pas être traitées ultérieurement pour des finalités incompatibles avec ces finalités. Ces finalités seront énoncées dans la clause/charte vie privée du responsable du traitement dont la personne concernée a connaissance au moment de la collecte de ses données personnelles.

Quid dès lors si une société entend exploiter pour un but de big data des données collectées antérieurement pour une finalité particulière et différente ?

L'entreprise devra se poser la question de la compatibilité de ce traitement ultérieur avec la finalité du traitement original.

Si le traitement ultérieur de big data ne semble pas compatible avec la finalité de départ, le traitement ultérieur peut encore se réaliser si ce traitement ultérieur est soit fondé sur le consentement de la personne concernée, soit sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23.1. du RGPD.

Si, le responsable du traitement ne peut se reposer sur l'une de ces deux exceptions, il pourra encore réaliser le traitement ultérieur mais il devra alors, pour se décider, tenir compte entre autres :

a) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;

b) du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;

c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10 ;

d) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;

e) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

La société peut également réaliser des traitements ultérieurs incompatibles avec les finalités initiales si ces traitements sont réalisés, entre autres, à des fins statistiques. Des garanties appropriées devront toutefois être mises en place.

b. *Le principe de minimisation des données*

L'autre grand principe qui posera énormément de souci en cas de traitements liés au big data est le principe de minimisation des données.

En effet, selon ce principe, les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Les données ne devraient être traitées que si la finalité du traitement envisagé ne peut être raisonnablement atteinte par d'autres moyens que par le traitement.

Une analyse au cas par cas doit être sérieusement effectuée par le responsable de traitement quant à savoir si toutes les données qu'il entend faire passer à la moulinette du big data sont réellement pertinentes, adéquates et utiles dans le cadre de ce traitement. Souvent, la finalité poursuivie pourra être atteinte autrement par des mesures plus respectueuses des droits des personnes concernées.

c. *Les principes d'exactitude et de limitation de la conservation*

Les principes d'exactitude (le responsable du traitement devra se soucier de ne traiter dans le cadre de son big data que des données exactes, et mises à jour) et de limitation de la conservation (les données ne peuvent être conservées permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées) sont aussi à tenir à l'œil.

Conformément au principe d'*accountability* (de responsabilité) de l'article 5.2 du RGPD, le considérant 91 du Règlement reprend l'hypothèse du big data pour conseiller au responsable du traitement de réaliser une analyse d'impact.

d. *Les bases juridiques*

Tout traitement doit reposer sur une des bases juridiques de l'article 6 du RGPD.

Un traitement big data devra se baser sur le consentement explicite de la personne concernée dans le cas où le traitement concerne (en tout ou en partie) des données particulières au sens de l'article 9 du RGPD (données de santé par exemple). Ce consentement explicite sera aussi requis dans le cas où le traitement big data est un traitement ultérieur au sens de l'article 6.4 du RGPD.

Dans le cas où les données qui entrent dans le traitement big data sont (en tout ou en partie) des données qui ont été collectées par un tiers, il faudra analyser si le traitement big data est compatible avec la finalité pour laquelle les données avaient été collectées par le tiers afin de voir si l'une des exceptions de l'article 6.4 du RGPD peut s'appliquer.

L'entreprise pourrait aussi réaliser un traitement big data si ce traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci (article 6.1.b du RGPD). Dans le cas où le traitement concerne des données particulières au sens de l'article 9, le traitement big data ne sera uniquement permis que s'il « est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale » (article 9.2.b du RGPD).

Quid de fonder le traitement big data sur les intérêts légitimes du responsable du traitement ?

Ce sera problématique pour le responsable du traitement. En effet, la personne concernée dispose ici d'un droit d'opposition (qu'il doit, il est vrai, fonder sur des raisons tenant à sa situation personnelle) et cette base de licéité ne vaut que pour les données non particulières au sens des articles 9 et 10 du RGPD.

e. *Profilage*

Le RGPD n'interdit pas du tout le profilage des personnes concernées, but premier généralement de toute utilisation de données massives. Le profilage est autorisé s'il est nécessaire à la conclusion ou à l'exécution d'un contrat ou si la société a obtenu le consentement explicite de la personne concernée.

Dans ces deux cas, la société devra mettre en œuvre des « mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision » (article 22.3 du RGPD).

Des traitements de profilage réalisés par l'intermédiaire du big data ne peuvent être fondées sur les catégories particulières de données à caractère personnel visées à l'article 9 du RGPD à moins qu'il y ait eu consentement explicite et que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient en place (article 22.4 du RGPD).

Il est dès lors clair que cette exigence de consentement limitera de façon claire les possibilités de profilage par une société.

En effet, dès que le traitement big data concerne (en tout ou en partie) des données particulières au sens de l'article 9 du RGPD, la société devra disposer du consentement explicite de la personne concernée. Rappelons que tout consentement doit être libre et donc exempt de toute pression de la part du responsable du traitement.

D. Les risques liés au big data (présentation sommaire)

Les données massives peuvent être utilisées pour identifier des corrélations et définir des tendances (commerciales ou autres) générales permettant de mieux comprendre une situation et ses évolutions.

Toutefois, elles peuvent également être traitées afin de décortiquer très finement et exhaustivement le comportement des individus. Les mêmes algorithmes et outils analytiques utilisés par un distributeur et un banquier pour comprendre les intérêts, les désirs des individus, et déterminer ce qu'ils peuvent lui vendre, peuvent être utilisé par un gouvernement, des partis politiques, des entreprises privées de sécurité pour calculer (et souvent mal calculer) si vous pouvez être une menace (exemple les fiches S français), maintenant ou dans l'avenir.

Ce ne sont pas les mégadonnées qui sont en elles-mêmes inquiétantes, mais bien les utilisations des résultats qui en découlent. La multiplication des capteurs qui a lieu via le développement de l'internet des objets (GPS, montres connectées, traceurs d'activité, domotique …), augmente considérablement les flux de données et les possibilités de percer de nombreux espaces qui étaient auparavant privés.

Des collectes de données peuvent ne pas sembler importantes par elles-mêmes.

Toutefois, lorsque les données enregistrées sont agrégées (comme la collecte de nos Likes sur Facebook qui peut permettre d'identifier notre comportement ou notre vie sociale), elles peuvent créer une image complète d'une personne. Ce qui peut potentiellement lui être extrêmement nuisible, en particulier lorsque cette analyse se trouve dans les mains de tiers non autorisés. Aujourd'hui, le risque que les gens perdent le contrôle de leurs propres données et de leur destin devient maximum.

Le big data mal géré peut donc mener à des extrêmes, à de fortes manipulations ou à de fausses prédictions (au travers de la science comportementale par exemple).

Plusieurs difficultés apparaissent :

- c'est tout d'abord la difficulté de choisir la bonne méthode, c'est-à-dire celle qui va donner les résultats que l'on cherche et qui correspond à la nature des données ;
- c'est ensuite la difficulté d'interpréter correctement les résultats. La facilité avec laquelle on obtient des résultats cache la complexité des méthodes employées ;
- la méthode d'observation est elle-même biaisée : un échantillon n'est représentatif que pour quelques critères. C'est une image faussée que

l'on observe, et augmenter indéfiniment la taille de l'échantillon, c'est le rapprocher plus de cette image faussée que de la réalité.

Le big data est aussi utilisé dans les projets développés dans le but de développer de meilleurs médicaments, de mieux gérer nos gigantesques villes, de rendre leurs politiques plus transparentes (généralisation de l'ouverture des données publiques – Open Data), de diminuer la violence urbaine (à travers la police prédictive surtout testée aux États-Unis), de développer les infrastructures urbaines et l'accès à internet un peu partout ainsi que de rendre les moyens de transport moins énergivores et plus respectueux de l'environnement. C'est l'ambition que nos villes deviennent des « *smart cities* », plus interactives.

Ces projets se développent en se basant sur les nouvelles technologies en ce compris l'internet des objets, des senseurs posés un peu partout, des caméras (postées sur des bâtiments ou sur des agents de police) voire des drones capables de réaliser de la surveillance et de la reconnaissance faciale et des plaques de voiture.

Ces ambitions vont rapidement se heurter à la problématique de la protection des données à caractère personnel : quelles données utiliser ? Comment être sûr de la valeur et de la qualité de ces données ? Comment être sûr que les données qui vont servir aux études ont été collectées en respectant la réglementation en place ? Comment vont-elles être conservées ? Qui aura accès aux données ? entre quelles autorités publiques et avec quelles sociétés commerciales nos données seront-elles partagées ? Comment être sûr que les principes de *privacy by default* et de *privacy by design* ont été bien respectés ? Voulons-nous vraiment être dirigés par ces prédictions automatiques même si le but peut être à première vue louable (diminuer les infractions et la violence par exemple) ?

De plus, la plupart du temps, les applications informatiques sont gérées par des sociétés privées qui poursuivent leur propre objectif de rentabilité et de profit. En matière de police prédictive, ces sociétés opposent leur secret professionnel aux chercheurs qui tentent de comprendre la complexité de leurs algorithmes.

La transparence et l'information correctes seront primordiales. Les citoyens sont en droit de connaître quand leurs données sont traitées, selon quels algorithmes et pour quels résultats possibles et avec quels contrôles. Il est aussi primordial que le choix des techniques et des fournisseurs de ces techniques se fasse en toute indépendance et efficience (analyse coûts *versus* efficacité) vu l'importance des données (de l'ensemble de la population d'une ville) qui risquent d'être partagées et des conclusions qui en sont tirées.

Les traitements opérés doivent être supervisés et contrôlés par l'autorité indépendante de contrôle des données personnelles nationale. L'autorité doit disposer des ressources suffisantes et du personnel adéquat dans le but d'analyser adéquatement et complètement l'impact des technologies utilisées qui traitent à grande échelle nos données à caractère personnel.

À l'ère de la digitalisation et du big data, de plus en plus d'entreprises utilisent aussi des algorithmes pour cibler les candidats pouvant correspondre à

un poste donné. Le « recrutement prédictif » permet d'analyser un large spectre de paramètres incluant notamment les traits de personnalité, les compétences, l'expérience, les facteurs de motivation et de satisfaction, les fiches de poste…

Plus précisément, les recruteurs vont savoir si tel ou tel trait de personnalité est le meilleur indicateur pour identifier la performance dans un poste donné ou encore si une expérience professionnelle permet de prédire avec plus de succès l'adéquation d'un candidat avec un environnement ou un poste de travail donné…

Pour des postes de front office, on identifiera les caractéristiques d'un candidat qui a le meilleur impact sur la satisfaction de la clientèle, etc.

Les services RH des entreprises espèrent que le recrutement prédictif va réduire le temps qu'on aurait pu consacrer à un recrutement classique, et diminuer le turn-over induit par les erreurs de casting.

Un dernier exemple que nous aimerions mettre en évidence est ce que l'on appelle la « justice prédictive ».

En résumé, il s'agit, dans un mouvement d'open data, de numériser des millions de décisions judiciaires afin de pourvoir les rendre publiques et les utiliser par après grâce au numérique et à des algorithmes. Les décisions rendues en matière civile et commerciale sont concernées mais pourquoi par après (sujet sensible et plus risqué), les décisions rendues en matière pénale.

Les décisions devront être bien sûr anonymisées un maximum tout en se posant deux questions : une totale anonymisation est-elle ici possible et quelles sont les données personnelles qu'il faut anonymisées ?

Il est clair que des start-ups (des *legal tech*) vont s'en saisir dans le but de rendre possible la prévision des décisions judiciaires par identification des juges ou des juridictions.

De réels enjeux inhérents à la sauvegarde de la vie privée et des libertés individuelles apparaissent. Et philosophiques car comment et pourquoi concevoir la nature humaine comme un agrégat de données qu'il convient de connaître, de configurer et d'analyser pour organiser la vie en société ?

Derrière ces « simples » questions s'en dissimulent d'autres : quel est le statut juridique de l'algorithme utilisé ? Quelle est sa place en procédure ? Comment encadre-t-on son usage ? Qui a construit l'équation ? Qui agrège les données ? Qui opère des audits ? Ne risque-t-on pas de favoriser un certain conformisme dans les décisions judiciaires ?

Ces enjeux sont considérables et à haute teneur anthropologique, de sorte qu'il ne saurait être question de les abandonner aux divers comités d'éthique que proposent certains acteurs privés.

De plus, dès l'instant où le magistrat, du siège ou du parquet, a recours à une équation mathématique pour administrer la preuve d'une faute civile ou pénale (la culpabilité), pour analyser des faits, construire un raisonnement, il faut alors que la magistrature ait accès à la nature et aux modalités d'agrégation des données soumises à l'équation algorithmique, comme à l'économie de

cette équation, pour pouvoir apprécier la rigueur, la qualité, l'impartialité de l'administration de la preuve. Seuls les régimes dictatoriaux s'affranchissent de ce principe.

Il est en effet essentiel d'acquérir dès le début la confiance des citoyens dans le développement des applications liées au big data.

E. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 25 : Droit 8 : Le droit à ne pas faire l'objet d'une décision automatique, y compris le profilage*
- *Fiche de guidance n° 42 : Le cloud computing et le RGPD*
- *Fiche de guidance n° 44 : le RGPD et le (direct) marketing*

Fiche de guidance n° 36
Les objets connectés et le RGPD

A. Introduction

Le RGPD a un impact considérable sur les entreprises dans toute l'Europe. La protection des données à caractère personnel est un défi qui concerne aussi les données collectées par les objets connectés (« *Internet of Things* » ou IoT).

Les entreprises vont devoir mieux maîtriser leur processus de collecte, d'intégration, de certification, de publication, de supervision et, bien entendu, de protection de toutes leurs données relatives aux personnes qu'elles possèdent qu'il s'agisse de leurs employés, clients et autres tiers.

Toutes les données transmises par un objet connecté peuvent être potentiellement considérées par défaut comme personnelles. D'où la nécessité de tenir compte dès le départ des principes de confidentialité. Et ce, dans les environnements des entreprises qui les vendent et utilisent et avec l'ensemble des fournisseurs impliqués dans la collecte, le stockage et le traitement des données.

Vient ensuite la question de la qualité, une problématique particulièrement urgente pour les organisations en phase de déploiement de leurs capacités de gestion de l'IoT. En effet, dans ce domaine, la volonté de limiter les coûts pousse souvent les organisations à faire avec des réseaux de qualité médiocre, ce qui peut affecter la qualité et la sécurité des données.

B. Difficultés du sujet

L'une des principales problématiques en la matière vient de l'existence dans les entreprises de silos de données difficiles à intégrer.

Prenons le cas où une entreprise disposerait d'informations sur un client à la fois issues de dispositifs IoT, d'applications de gestion telles des ERP (SAP) ou des applications de gestion de la relation client et d'applications de marketing.

En cas de demande d'une personne concernée, l'entreprise serait alors tenue de lui fournir l'ensemble de ses données privées le concernant, comme l'exige RGPD. Les entreprises devront donc rapprocher l'ensemble de leurs informations, y compris celles provenant des objets connectés. Pour les entreprises qui ignorent où se trouvent les données qu'elles ont collectées et qui en est responsable, tenir le délai d'un mois risque d'être impossible.

Avec le développement des nouvelles technologies, les objets connectés vont se multiplier (six par personne à l'horizon 2020, selon diverses études). Les maisons vont être de plus en plus connectées. Cette nouvelle masse d'informations va révéler de plus en plus de choses sur les utilisateurs. Sans compter les progrès de l'intelligence artificielle qui va permettre de dresser le profil psychologique d'un individu à partir des simples publications qu'il poste sur son compte Twitter.

Fiche de guidance n° 37
ePrivacy

A. Introduction

Le RGPD réglemente la protection des données à caractère personnel. Il remplace la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. La directive 2002/58/EC du 12 juillet 2002 (directive vie privée et communications électroniques) (modifiée en 2009) est venue compléter la Directive de 1995 en précisant les règles de protection de la vie privée dans le secteur des communications électroniques.

Dès lors, après avoir mis à jour les règles initiales de la Directive de 1995, il était logique que la Commission européenne fasse de même pour les règles contenues dans la Directive de 2002. C'est le but de la proposition de Règlement publié par Commission européenne le 10 janvier 2017. Nous appellerons ce texte la proposition de Règlement *ePrivacy* par la suite.

La réforme est nécessaire et salutaire.

En effet, la directive de 2002 ne s'applique pas aux nouvelles formes de communication, à la convergence des médias, aux réseaux sociaux et à la communication machine à machine.

La proposition de la Commission voudrait, en tant que *lex specialis* au RGPD, adapter (e.a.) :

1. les règles relatives aux cookies (qui visent à cibler les internautes), aux coups de téléphone et aux emails de marketing direct ;
2. les restrictions qui s'appliquent aux fournisseurs de communications électroniques.

Le RGPD s'appliquerait dans tous les cas de figure sauf dans la matière de la *ePrivacy* où la proposition de Règlement s'appliquerait. Toutefois, il serait bon d'avoir des clarifications dans le Règlement *ePrivacy* afin de bien savoir dès

le début quand le RGPD s'applique et quand ce serait au tour du Règlement *ePrivacy* de s'appliquer.

La proposition de Règlement s'applique aux nouvelles formes de services proposant des communications électroniques comme les messageries instantanées, les services de VOIP, les *web-based emails*, les communications machine à machine et les appareils connectés (« IoT »).

Il y a toutefois une grande différence entre la proposition de Règlement *ePrivacy* et le RGPD. Le RGPD est basé sur l'article 8 de la Charte des Droits Fondamentaux protégeant les données tandis que la ePrivacy est basée sur son article 7 protégeant la confidentialité de la vie privée.

Par exemple, en matière de vie privée, il ne peut y avoir des intérêts légitimes permettant des intrusions dans la vie privée.

B. Réactions

Pour beaucoup, la proposition de nouvelle réglementation n'est pas adaptée aux évolutions technologiques. En effet, elle s'attaque aux cookies alors que les entreprises peuvent cibler directement les utilisateurs sur leur téléphone, leur ordinateur, leur tablette sans avoir besoin des cookies. Et ce n'est que le début : l'intelligence artificielle va permettre de reconnaître les individus par des moyens de moins en moins détectables.

Le Contrôleur européen de la protection des données de Butarelli a écrit une opinion très critique sur la proposition de Règlement *ePrivacy* (« *EDPS Opinion 06/2017 of 24 April 2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*).

Le Parlement européen a lui demandé qu'une étude soit réalisée de la proposition de Règlement. L'étude a été finalisée en mai 2017 par l'IviR, l'« *Institute for Information Law, University of Amsterdam* » (« *An assessment of the Commission's Proposal on Privacy and Electronic Communications – Study for the LIBE Committee* »).

Le Groupe de Travail « Article 29 » a aussi émis une opinion très critique sur la proposition de Règlement (WP 247 du 4 avril 2017). Le Groupe de Travail « Article 29 » reconnaît l'importance du sujet.

Il reconnaît comme une très bonne avancée le fait d'avoir choisi l'instrument du Règlement plutôt que de la directive pour tenter d'harmoniser au mieux les différentes législations nationales.

Toutefois, le Groupe de Travail « Article 29 » critique la proposition de Règlement *ePrivacy* sur 4 points d'attention majeurs qui, selon lui, diminuent les protections offertes par le RGPD :

1. le traçage (« *tracking* ») des données de localisation des « *terminal equipment* » (il s'agit des éléments susceptibles d'échanger des

données avec un réseau mais qui ne se connectent pas directement à la ligne de transmission. Par exemple : un ordinateur, un terminal, une imprimante…) ;

2. les conditions des autorisations permettant d'analyser le contenu des communications et des métadonnées ;
3. les conditions d'utilisation (les « *settings* ») par défaut des « *terminal equipment* » et des logiciels ;
4. les « *tracking walls* », le fait de devoir donner son consentement à ce que les données du visiteur d'un site web (d'un journal) soient collectées et traitées pour des finalités de traçage et de publicités ciblées afin de pouvoir accéder audit site.

C. Parlement européen

Le 9 juin 2017, la parlementaire Marju Lauristin de la Commission « *Civil Liberties, Justice and Home Affairs* » du Parlement européen a publié un projet de rapport. Il s'agit de la commission au Parlement européen en charge de délivrer le rapport au nom du Parlement européen, tout en tenant compte des rapports d'autres commissions qui s'étaient aussi saisis de la question.

Le projet de rapport durcit le régime proposé par la Commission européenne en janvier 2017 en proposant plus de restrictions en matière marketing direct et sur les utilisations possibles des données de communication.

Les points d'attention du projet de rapport sont les suivants :

1. le Règlement *ePrivacy* ne peut avoir comme conséquence que les règles de protection du RGPD soient modifiées vers le bas.

   Le Règlement *ePrivacy* devrait « juste » apporter y apporter des règles complémentaires et des précisions nécessaires ;
2. dans un but d'augmenter l'harmonisation européenne, le projet de rapport supprime la possibilité pour les États membres d'introduire des règles supplémentaires ;
3. le Règlement *ePrivacy* devrait contenir toutes les définitions qui sont nécessaires à sa parfaite compréhension.

   Il est inutile de renvoyer par exemple vers le (futur) Code des communications électroniques européennes ;
4. le projet de Rapport limite encore plus les fondements juridiques pour traiter le contenu des communications ainsi que leurs métadonnées.

   Par exemple, lorsque la base juridique est le consentement, la proposition précise que dorénavant le consentement des deux parties à la communication (celui qui a émis la communication et celui qui

doit la recevoir) doit être obtenu (ce qui pourrait être difficile dans la pratique) ;

5. toutefois, l'extension des règles vers les fournisseurs que l'on appelle « *over-the-top* » (« OTT ») (comme Skype, WhatsApp, Facebook Messenger, Gmail, Viber, Snapchat) est maintenue.

   Rappelons que si le Règlement est adopté, ces fournisseurs seront soumis aux mêmes règles que Proximus ou Base ;

6. le projet de rapport propose une autre définition de ce qu'il faut comprendre par « metadata » = « tout ce qui n'est pas du contenu ».

   Toutefois, cela pose la question de savoir ce qu'est du « contenu » ;

7. tout comme le Groupe de Travail « Article 29 » dans son analyse, le projet de rapport interdit expressément de devoir donner son consentement avant de pouvoir utiliser un service ou un site internet.

   La seule exception permise serait lorsque le traçage de l'utilisateur est nécessaire pour la fourniture du service. Toutefois, cette exception serait interprétée de manière très restrictive ;

8. le projet de rapport ajoute que même les communications de machine à machine doivent rester confidentielles mais uniquement quand cette communication concerne une personne ;

9. le projet de rapport clarifie le fait que toute interférence avec des données de communication est interdite, que les données soient au repos ou en transit (confidentialités des données) ;

10. déterminer la localisation d'un utilisateur ou collecter d'autres informations émises par l'appareil de l'utilisateur grâce au Wi-Fi, Bluetooth ou des technologies similaires serait uniquement permis avec l'autorisation de l'utilisateur (en ligne avec les considérations du Groupe de Travail « Article 29 ») ;

11. les fournisseurs de service de communication peuvent, pour l'instant, traiter les données de communication si cela est nécessaire pour les communications ou pour organiser la facturation ou pour des finalités liées à la livraison du service (« *service delivery purposes* »).

    Ces possibilités seraient restreintes : les données pourraient être traitées uniquement si leurs traitements est strictement nécessaire, ou, s'il s'agit de contenu, si c'est techniquement strictement nécessaire pour le service ;

12. tous les traitements des données de communication par les fournisseurs des services de communication sont strictement interdits à moins que le Règlement *ePrivacy* permette leur traitement ;

13. la possibilité pour les fournisseurs de service de communication de rendre anonymes les données quand les données ne sont plus nécessaires est supprimée. Les données devront, à la place, être supprimées ;

14. les fournisseurs de navigateurs sur internet (« *browsers* ») et les systèmes d'exploitation (les « *operating systems* ») doivent s'assurer, de par l'application du principe de *privacy by design*, que le traçage et les possibilités de récolte automatique de données sont mises sur off.

    Les utilisateurs devraient d'eux-mêmes activer ces technologies. Leur choix devrait être transmis aux parties tierces qui devraient les respecter. À ce sujet, la proposition du rapport a une vision très différente de celle de la proposition de Règlement. En effet, la proposition de Règlement de la Commission européenne considère comme suffisant que les « *browsers* » aient des options en matière de *privacy* mais il ne faut pas que ces options empêchent d'office dès l'installation du *browser* toute possibilité de *tracking* ;

15. dans le cas où les fournisseurs de service de communication cryptent les communications, le décryptage des données ou toute tentative de modifier la sécurité des fournisseurs est interdite (interdiction pouvoir permettre que les autorités puissent avoir la possibilité de décrypter les messages pour des raisons de sécurité pour éviter toute surveillance de masse (interdiction des « *backdoors* ») (art. 11 de la proposition de Règlement) ;

16. la proposition de rapport exige que l'ensemble des pays européens crée des *Do-Not-Call Lists* afin de permettre aux citoyens européens qui le désirent de s'y inscrire pour ne plus subir les actions de marketing par téléphone.

17. Les sociétés devraient obligatoirement nettoyer leur liste d'envoi de marketing avant d'entreprendre une campagne marketing téléphonique. Les *Do-Not-Call List* existent déjà dans plusieurs pays européens (dont la Belgique);

18. les sociétés qui offrent des services dans l'UE mais qui n'y sont pas établies doivent désigner un représentant européen.

19. Cette obligation s'applique aux fournisseurs de services de communication électronique et aux fournisseurs de logiciels permettant des communications électroniques, des sociétés envoyant des communications de marketing direct et des sociétés collectant des informations à propos d'un appareil d'un utilisateur ;

20. la proposition de rapport introduit la possibilité pour les utilisateurs de mandater des organisations non commerciales pour introduire une plainte en leur nom.

D. Prochaines étapes

La publication du projet de rapport ne fut pas la fin du processus législatif. Loin de là.

Les parlementaires devaient faire parvenir à Lauristin leurs amendements pour le 10 juillet 2017. Lauristin demanda aussi au service juridique du Parlement européen des précisions quant au champ d'application de la proposition de Règlement en tant que *lex specialis* par rapport au RGPD.

Lauristin (ayant gagné des élections locales en Estonie) a quitté pendant le déroulement des travaux le Parlement européen. Elle a été remplacée par Mme Sippel.

La commission LIBE du Parlement européen a rendu son rapport final en octobre 2017. Le rapport fut voté 31 votes contre 24 (et une abstention). Le Parlement européen a, par après, adopté le rapport Lauristin.

Comme pour tout texte législatif européen, le Conseil de l'UE doit aussi adopter ses propres amendements. Rappelons qu'une fois que le Parlement européen et le Conseil de l'UE ont défini leur position, ils devront négocier le texte final du Règlement ensemble avec la Commission européenne (dans le cadre du fameux « trilogue européen » opaque et totalement non transparent auquel nous ne souscrivons aucunement mais qui devient la procédure normal d'adoption des textes européens).

Voici un aperçu des grandes lignes du rapport Lauristin voté en octobre 2017.

Ces modifications, si elles sont reprises dans le texte définitif, vont obliger les Google et Facebook à modifier leur manière de travailler en Europe et de traiter les données issues de citoyens européens :

- les bandeaux de cookies vont disparaître.

  À la place, le texte prévoit que les navigateurs devront inclure une désactivation par défaut des cookies tiers. L'internaute devra définir ses préférences dans les paramètres de confidentialité : soit tout bloquer, tout accepter ou alors une solution intermédiaire. Un choix qui s'appliquera ensuite à tous les sites visités. Une solution combattue farouchement par les éditeurs de presse qui auront beaucoup plus de mal à gérer l'identification des surfeurs, la personnalisation des contenus et la segmentation des publicités ;
- le consentement éclairé d'une personne devra être obtenu préalablement dans le cas où son appareil serait pisté/tracké via des cookies, une mise à jour logicielle ou des hotspots Wi-Fi dans des centres commerciaux. Dans le cas contraire, ces pratiques seraient interdites ;
- les paramètres de « confidentialité par défaut » doivent devenir la norme pour tous les logiciels utilisés pour les communications électroniques et les fournisseurs de services ont pour mission de prévoir un chiffrement fort ;

- les données ne pourront être utilisées que dans le but pour lequel le consentement aura été donné par l'individu. Quant aux métadonnées, elles sont désormais considérées comme confidentielles et ne doivent jamais être transmises à des tiers. Quid dès lors du *tracking* comportemental et des publicités ciblées ? ;
- interdiction du fait d'obliger les internautes à accepter les cookies de traçage avant d'accéder à un site web ;
- toutefois, l'utilisation de ces cookies serait autorisée sans notre consentement pour « mesurer l'audience du site » (Google Analytics).

Les acteurs des médias européens ont souligné les conséquences sur l'économie d'Internet et le pluralisme de l'information en Europe des règles proposées.

En effet, leur mise en œuvre pourrait impliquer un avantage inédit et décisif en matière de collecte de données personnelles offert aux fameux Gafa (Google, Amazon, Facebook, Apple) en privant les médias des cookies et donc des publicités ciblées. Ce qui mettrait en danger leur modèle économique.

Pour utiliser des services comme Facebook, Android, Gmail ou Amazon, il faut s'inscrire, décliner son identité, puis accepter les conditions générales, qui incluent l'autorisation de collecte et d'exploitation des données personnelles.

Les Gafa seraient donc les seuls acteurs de l'Internet en Europe en mesure de collecter massivement les données personnelles et de les exploiter à des fins publicitaires. En faisant disparaître les cookies, l'Europe risque de réduire le marché publicitaire aux seuls acteurs du Web qui collectent des données sans passer par les cookies.

La Commission européenne considère quant à elle que le choix de bloquer au niveau du navigateur tous les traceurs « ne prive pas les exploitants de sites Web de la possibilité d'obtenir un consentement par l'envoi de demandes individuelles aux utilisateurs finaux et donc de conserver leur modèle économique actuel ».

La Commission européenne avait annoncé vouloir que le Règlement soit finalisé pour mai 2018 (au moment de l'entrée en vigueur du RGPD). Toutefois, il semble qu'aujourd'hui, ce délai soit irréaliste. Le processus législatif risque en effet de se terminer bien après !

Fiche de guidance n° 38
Principales différences entre le RGPD et la Directive de 1995

A. Introduction

Le RGPD ne modifie pas fondamentalement les règles principales de la matière qui étaient déjà présentes dans la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Par exemple, le RGPD reprend de la directive la majorité de ses définitions.

Le RGPD étend significativement les règles en introduisant de nouvelles exigences fondées sur ces principes généraux déjà existants.

B. Comparaison Directive – Règlement : Tableau

Les différences sont pourtant nombreuses. Marquons ici les principales.

Directive	Règlement
Texte devant être transposé par les États membre	Texte obligatoire sans avoir à être transposé mais qui nécessite pourtant beaucoup de précisions étatiques
Texte comportant 72 considérants et 34 articles	Texte comportant 173 considérants et 99 articles
	Importance exacerbée des considérants
	Trois fois plus de définitions
	Même si le champ d'application matériel est identique, la définition de ce que l'on entend par « donnée personnelle » est plus complète (reprenant en exemple les adresses IP)

	Champ d'application territorial étendu aux sociétés situées hors UE qui visent des clients européens
	Ajout de nouveaux principes généraux : transparence, limitation des finalités, minimisation des données et garantie de sécurité
	Définition plus précise du consentement
	Précisions supplémentaires quant aux conditions des traitements
	Précisions pour des traitements ultérieurs compatibles
	Précisions quand le traitement concerne un enfant
	Changement de terminologie pour les données sensibles
	Nouvelles précisions quant aux données sensibles
	Précisions concernant la transparence des informations et des communications et les modalités de l'exercice des droits de la personne concernée
	L'exercice des droits est dorénavant gratuit
Droit d'information concerne 5 types d'information	Droit d'information concerne 12 types d'information
	Nouveaux droits pour la personne concernée : droit à la portabilité
Déclaration aux autorités de contrôle de protection des données personnelles avant tout traitement	Suppression des déclarations aux autorités de contrôle de protection des données personnelles et création d'un registre des traitements internes
	Reconnaissance de la possibilité d'une responsabilité conjointe du traitement lorsque deux responsables du traitement (ou plus) déterminent conjointement les finalités et les moyens du traitement
	Précisions en matière de transfert hors UE
	La notification aux autorités de contrôle de protection des données personnelles en cas de violation des données à caractère personnel
	Règles supplémentaires concernant les contrôles de protection des données personnelles
	Règles supplémentaires concernant la coopération entre les autorités de contrôle de protection des données personnelles
	Règles relatives à l'établissement de l'autorité de contrôle
	Mise en place de règles relatives à la Coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées
	Création du Mécanisme de contrôle de la cohérence
	Création du Comité européen de la protection des données
Inexistant	Le montant des amendes

Fiche de guidance n° 39
Un Règlement ?
Non, une Règlective plutôt !

A. Principe

Pour les sociétés qui opèrent de manière transfrontière, l'harmonisation opérée par le RGPD est la bienvenue.

Toutefois, des divergences nationales risquent d'apparaître ou de subsister pour longtemps. En effet, les États membres ont le pouvoir d'amender/compléter certaines des obligations qui découlent du RGPD.

B. Tableau

Il y a plus de cinquante renvois aux législations nationales dans le règlement dont plusieurs qui concernent la santé ou le secteur public. Le RGPD contient aussi des possibilités laissées aux États membre, possibilités que les États membre peuvent ou pas introduire dans leur législation (dans le jargon, on appelle cela « lever une option ») :

• sécurité nationale • défense nationale • sécurité publique • prévention et détection d'infractions pénales • autres objectifs importants d'intérêt public général de l'Union ou d'un État membre (notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale) • protection de l'indépendance de la justice et des procédures judiciaires • prévention et détection de manquements à la déontologie des professions réglementées • mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique • protection de la personne concernée ou des droits et libertés d'autrui • exécution des demandes de droit civil (article 23 du RGPD)	limitation des droits issus du RGPD et des principes généraux de l'article 5 du RGPD
concernant la licéité du traitement (article 6.2 du RGPD)	les États membre peuvent maintenir ou introduire des dispositions plus spécifiques déterminant plus précisément les exigences spécifiques applicables au traitement nécessaire : • au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou • à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement
concernant les conditions applicables au consentement des enfants (article 8 du RGPD)	en ce qui concerne les services de la société de l'information
concernant le traitement portant sur des catégories particulières de données à caractère personnel (article 9.4 du RGPD)	données génétiques, biométriques ou concernant la santé
concernant la réalisation des analyses d'impact (les AIPD) (article 36.5 du RGPD)	en ce qui concerne la consultation préalable des autorités de contrôles
concernant les missions du DPD	les États membres peuvent en rajouter) (voyez le « au moins » de l'article 39.1 du RGPD)
autorités de contrôles nationales (article 51 et s. du RGPD)	concernant les conditions générales applicables à l'organisation des autorités de contrôle et par exemple à la nomination des membres des autorités de contrôle
concernant la représentation des personnes concernées (article 80 du RGPD)	possibilité pour les États membres de prévoir que leur Test-Achat national peut introduire une réclamation lorsque l'association considère que les droits d'une personne concernée ont été violés du fait d'un traitement
traitement et liberté d'expression et d'information (article 85 du RGPD)	les États membre doivent concilier, par la loi, le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire

traitement du numéro d'identification national (article 87 du RGPD)	les États membre peuvent préciser les conditions spécifiques du traitement d'un numéro d'identification national ou de tout autre identifiant d'application générale
traitements de données dans le cadre de la relation de travail (article 88 du RGPD)	les États membre peuvent introduire des restrictions supplémentaires lorsqu'il s'agit de traitements de données relatives à des employés
traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques (article 89 du RGPD)	lorsque des données à caractère personnel sont traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, le droit de l'Union ou le droit d'un État membre peut prévoir des dérogations aux droits des personnes concernées
contrôle des traitements et respect du secret (article 90 du RGPD)	les États membre peuvent adopter des règles spécifiques afin de définir les pouvoirs des autorités de contrôle à l'égard des responsables du traitement ou des sous-traitants qui sont soumis, en vertu du droit de l'Union ou du droit d'un État membre ou de règles arrêtées par les organismes nationaux compétents, à une obligation de secret professionnel ou à d'autres obligations de secret équivalentes, lorsque cela est nécessaire et proportionné pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret
etc.	

C. Conclusion

Outre ces dizaines de dérogations nationales possibles, il faut reconnaître que le texte en soi est parfois difficile à comprendre.

Le passé social et culturel de chaque État membre vont faire en sorte que les incompréhensions du texte vont être à chaque fois interprétée différemment ici et là. Ce qui est regardé comme « hauts risques » à Berlin ne le sera certainement pas à Rome.

Le travail des DPD des entreprises n'en sera que plus difficile. Ils vont devoir suivre, comprendre et analyser les implications pour leur société de chacun des textes publiés par le futur CEPD mais aussi par chacune des autorités de contrôle nationales. Chaque interprétation nationale pourra en effet servir de base à une argumentation dans un autre pays. C'est la force d'attraction d'un Règlement européen.

Il serait curieux de voir si un juge belge reprendra dans son argumentation une partie d'une décision portugaise arguant qu'il s'agit d'un Règlement à interprétation normalement paneuropéenne et donc uniforme pour l'ensemble des millions de citoyens européens.

Déjà des cabinets d'avocats compilent les différences entre les transpositions nationales afin d'aider leurs clients internationaux. La cartographie sera fort utile dans le futur.

Nous sommes aussi persuadés que la Cour de justice de l'Union européenne aura fort à faire dans quelques années lorsque les premières questions relatives aux incompréhensions (et elles sont nombreuses) reprises dans les milliers de mots du RGPD arriveront à son greffe.

À côté de tribunaux spéciaux pour le droit des marques et le droit des brevets, peut-être faudra-t-il bientôt mettre en place aussi un tribunal relatif à la protection des données à caractère personnel des citoyens européens ? Une suite qui semblerait tout aussi logique. Une juridiction européenne qui travaillerait en étroite collaboration avec les services de la concurrence de la Commission européenne et qui jugerait des abus des Google, Amazon, Facebook, Apple et autres Microsoft en matière de protection des données à caractère personnel.

D. Une directive qui ne dit pas son mot ?

Pour finir, nous aimerions faire un rapprochement entre le RGPD et ce que l'on appelle la Directive Info-Soc.

Il s'agit de la Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

Cette Directive en matière de droit d'auteur et de droits voisins a tenté de moderniser la matière de la propriété intellectuelle. Son texte comporte un article 5 reprenant, sous des termes vagues et donc au contenu flou, toute une liste d'exceptions aux droits des auteurs et des titulaires de droits voisins. La liste est exhaustive (les États membre ne peuvent imaginer une exception qui ne serait pas dans la liste des exceptions de l'article 5) mais pas obligatoire (les Etats membre ne sont pas obligés de reprendre toutes les exceptions mentionnées).

En d'autres mots, cette liste est à la carte.

Il va sans dire que les États membre s'en sont donné à cœur joie et que la Directive a complètement dès lors manqué son objectif de créer un « cadre juridique harmonisé du droit d'auteur et des droits voisins » (considérant 4). Aucune situation nationale n'est la même ! Beaucoup regrettent le fait que la liste de l'article ne soit pas exhaustive et obligatoire.

Nous craignons qu'en matière de protection des données personnelles, la situation ne devienne équivalente (ou du moins n'évolue pas plus vers une réelle harmonisation du sujet car rappelons que la Directive de 1995 en son article 13 prévoyait déjà toute une série d'exceptions et de limitations possibles pour des raisons vagues et générales) suite aux diverses possibilités de

dérogations permises par le RGPD et que nous n'avons qu'exemplifiées dans notre tableau.

Le travail de titan des différents parlementaires européens (dont Jan Philipp Albrecht qui fut l'excellent rapporteur du texte au niveau du Parlement européen) (nous ne pouvons que conseiller la vision du reportage télévisé qui rend compte du travail exemplaire qu'il fournit à l'époque) n'aura alors servi à rien.

Fiche de guidance n° 40
Le RGPD et la Directive NIS

A. Introduction

La Directive NIS (acronyme de « Network and Information Security ») est la Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Elle comporte 75 considérants et 27 articles. Elle est également le fruit de longues discussions (trois ans de négociations).

Cette directive (d'harmonisation minimale) est entrée en vigueur en août 2016. Les États membres ont 21 mois pour la transposer (avant mai 2018 donc) et 6 mois de plus pour identifier les « opérateurs de services essentiels » (les OSE). À ce jour, nous ne disposons pas encore du texte de transposition belge alors que la France vient de voter le sien (refrain connu).

B. Renforcer la capacité de résistance de l'UE aux attaques informatiques

La Directive NIS établit des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne afin d'améliorer le fonctionnement du marché intérieur.

À cette fin, la directive :

1. fixe des obligations à tous les États membres en ce qui concerne l'adoption d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;
2. institue un groupe de coopération afin de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance mutuelle ;

3. institue un réseau des centres de réponse aux incidents de sécurité informatiques (ci-après dénommé « réseau des CSIRT ») afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération rapide et effective au niveau opérationnel ;
4. établit des exigences en matière de sécurité et de notification pour les OSE et pour les fournisseurs de service numérique (FSN) ;
5. fixe des obligations aux États membres pour la désignation d'autorités nationales compétentes, de points de contact uniques et de CSIRT chargés de tâches liées à la sécurité des réseaux et des systèmes d'information.

En effet, suite à la Directive, chaque État membre devra prendre des mesures afin de promouvoir la sécurité informatique :

- chaque État membre devra disposer d'un *Computer Security Incident Response Team* (CSIRT) et d'une autorité nationale en la matière ;
- comme dit plus haut, il sera créé un centre de coopération dans le but de supporter et de faciliter la coopération stratégique ainsi que l'échange d'information entre les État membre.

  Il sera aussi créé un CSIRT Network pour promouvoir une coopération rapide et efficace entre les États membre lorsque des incidents de sécurité informatique se produisent ;
- doit se développer une culture de la sécurité informatique dans les secteurs qui sont considérés comme vitaux pour notre économie et notre société et qui font appel de manière très importante à l'informatique comme les secteurs de l'énergie, du transport, de l'eau, bancaire, des infrastructures de marchés financiers, de la santé et des infrastructures numériques (voir la définition de ces secteurs, sous-secteurs et types d'activités à l'Annexe 2 de la directive).

  Les sociétés actives dans ces secteurs qui ont été qualifiées par les États membre comme OSE devront prendre des mesures de sécurité adéquates. Elles devront aussi notifier les incidents sérieux aux autorités nationales compétentes. Les FSN (les moteurs de recherché, les fournisseurs de *cloud computing services* et les places de marché en ligne) devront satisfaire aux mêmes exigences en matière de notification et de sécurité. Une place de marché en ligne permet aux consommateurs et aux professionnels de conclure des contrats de vente ou de service en ligne avec des professionnels.

C. Obligations pour les États membres

Les États membre auront jusqu'au 9 novembre 2018 pour identifier au sein de chaque secteur et sous-secteur visé à l'annexe II de la directive, les OSE ayant un établissement sur leur territoire.

À intervalles réguliers et au moins tous les deux ans à compter du 9 mai 2018, les États membres devront procéder au réexamen et, au besoin, à la mise à jour de la liste des OSE identifiés préalablement.

Un OSE est :

a) une entité qui fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques

b) dont la fourniture du service est tributaire des réseaux et des systèmes d'information et

c) pour lequel un incident aurait un effet disruptif important sur la fourniture dudit service.

Chaque État membre devra établir une liste des services qui sont essentiels au maintien d'activités sociétales et/ou économiques critiques. Les États membre devront communiquer à la Commission européenne cette liste.

Au plus tard le 9 novembre 2018, puis tous les deux ans, les États membres devront communiquer à la Commission les informations qui lui sont nécessaires pour évaluer la mise en œuvre de la directive, en particulier la cohérence des approches adoptées par les États membre pour l'identification des OSE.

Les informations communiquées devront comprendre au moins :

a) les mesures nationales permettant l'identification des OSE ;

b) la liste des services qui sont essentiels au maintien d'activités sociétales et/ou économiques critiques ;

c) le nombre des OSE identifiés pour chaque secteur visé à l'annexe II de la directive et une indication de leur importance pour ce secteur ;

d) les seuils, pour autant qu'ils existent, permettant de déterminer le niveau de l'offre pertinent en fonction du nombre d'utilisateurs tributaires de ce service visé à l'article 6.1.a de la directive ou de l'importance de cet opérateur de services essentiels particulier visée à l'article 6.1.f.

Afin de contribuer à la transmission d'informations comparables, la Commission pourra, en tenant le plus grand compte de l'avis de l'Agence européenne chargée de la sécurité des réseaux et de l'information (l'ENISA), adopter des lignes directrices techniques appropriées concernant les paramètres applicables à ce type d'informations.

La directive NIS fait mention d'une série de secteurs au sein desquels les États membres devront identifier des OSE.

Ces secteurs sont les suivants :

1. Énergie : concerne les sous-secteurs de l'électricité, du pétrole et du gaz ;
2. Transports : concerne les sous-secteurs des transports aérien, ferroviaire, routier, et par voie d'eau ;
3. Banques : la directive désigne ainsi les établissements de crédit, entendu comme « une entreprise dont l'activité consiste à recevoir du public des dépôts ou d'autres fonds remboursables et à octroyer des crédits pour son propre compte » ;
4. Infrastructures de marchés financiers : concerne tout autant les exploitants de plate-forme de négociation que les contreparties centrales ;
5. Santé : concerne tout établissement de soins de santé, y compris les hôpitaux et cliniques privées ;
6. Fourniture et distribution d'eau potable ;
7. Infrastructures numériques : il s'agit des IXP (*Internet eXchange Point* ou « points d'échange internet »), définis comme « une structure de réseau qui permet l'interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l'échange de trafic internet », des fournisseurs de services DNS et des registres de noms de domaines de haut niveau.

D. Des impacts importants aussi pour les entreprises

Pour les entreprises, elle introduit deux volets d'obligation pour deux types d'acteurs :

1. les OSE (comme les banques) et
2. les FSN (comme les services d'informatique dans le cloud)

qui doivent mettre en œuvre des mesures techniques et organisationnelles pour gérer les risques menaçant la sécurité des réseaux et des systèmes d'information (peu importe si ces réseaux ou systèmes traitent des données à caractère personnel). Ces deux acteurs seront aussi tenus de notifier les incidents de sécurité à l'autorité compétente.

Toutefois, les micros entreprises et les petites entreprises ne sont pas concernés au sens de la recommandation 2003/361/CE (PME = moins de 50 ETP, et moins de 10 Mios € de CA).

La directive précise quand même que « les entités qui n'ont pas été identifiées en tant qu'opérateurs de services essentiels et qui ne sont pas des fournisseurs de service numérique peuvent notifier, à titre volontaire, les incidents ayant un impact significatif sur la continuité des services qu'elles fournissent. ».

E. Groupe de coopération

Le groupe de coopération aidera les États membres à suivre une approche cohérente dans le processus d'identification des OSE.

F. Que doivent faire les sociétés afin de satisfaire à la directive NIS ?

1. Comprendre que la sécurité informatique ne doit pas seulement être vue comme un problème IT

Les responsables les plus élevés de la société doivent être dorénavant conscients des risques informatiques liés aux activités de leur société.

Les CEO et CFO doivent être capables de répondre aux questions suivantes :

- quelles sont les principales vulnérabilités informatiques de ma société ?
- quelles sont les stratégies possibles pour diminuer ces risques ?
- avons-nous déjà mis les bonnes personnes pour traiter de ces problèmes ?

2. Une analyse des vulnérabilités/des risques est essentielle

Chaque société devrait réaliser sa propre analyse et ce en fonction d'un standard reconnu en la matière. Chaque société devrait être consciente de ses équipements informatiques. La société en est-elle propriétaire ou non ? Est-t-elle bien consciente des risques financiers d'une violation de ses réseaux à large échelle ?

Les mesures de sécurité à prendre par les OSE et les FSN devront couvrir les éléments suivants (nous retrouvons et ce n'est pas un hasard le même vocabulaire que celui du RGPD) :

1. la prévention des risques grâce à des mesures techniques et organisationnelles appropriées et proportionnées aux risques ;
2. assurer la sécurité des réseaux et des systèmes d'information : les mesures doivent assurer un niveau de sécurité proportionnel aux risques que présentent le réseau et les systèmes d'information concernés ;

3. gestion des incidents : les mesures doivent prévenir et minimiser l'impact des incidents sur les systèmes d'information utilisés pour fournir les services.

3. Le risque informatique est devenu une problématique des conseils d'administrations

Les régulateurs nationaux et européens vont mettre de plus en plus de pression sur les sociétés afin qu'elles soient dorénavant conscientes de leurs risques informatiques. Il ne faudra pas longtemps avant que les conseils d'administrations requièrent d'utiliser comme standard une identification à multiples facteurs, d'implémenter à chaque fois les derniers updates de sécurité et de réaliser des analyses de risques sur les fournisseurs habituels de la société. Il ne plairait pas à votre conseil d'administration de se rendre compte qu'il faut trois fois plus de temps à la société pour se rendre compte qu'elle a été victime d'une intrusion informatique qu'un concurrent.

4. Les sociétés vont devoir communiquer plus

Les incidents informatiques vont devenir de plus en plus d'actualité en Europe d'ici quelques temps. C'est dès à présent que les sociétés doivent se préparer à communiquer à ce sujet avec les différents régulateurs et autorités de contrôle. Et à engager les meilleurs experts informatiques.

En effet, tout comme pour les violations de données à caractère personnel, les OSE et les FSN devront notifier à leur autorité compétente ou au CSIRT, sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent. Les notifications contiennent des informations permettant à l'autorité compétente ou au CSIRT de déterminer si l'incident a un impact au niveau transfrontalier ainsi que son ampleur.

Afin de déterminer l'ampleur de l'impact d'un incident, l'OSE devra prendre en considération les paramètres suivants :

- le nombre d'utilisateurs touchés par la perturbation du service essentiel ;
- la durée de l'incident ;
- la portée géographique eu égard à la zone touchée par l'incident.
- Afin de déterminer l'importance de l'impact d'un incident, le FSN devra tenir compte en plus des éléments suivants :
- la gravité de la perturbation du fonctionnement du service ;
- l'ampleur de l'impact sur les fonctions économiques et sociétales

Le RGPD parle lui de risques élevés en exigeant que les responsables du traitement prennent en considération les conséquences pour les droits et libertés des personnes concernées.

L'un des points de débats précédant la publication de la directive NIS, concernait le périmètre et le contenu des notifications d'incidents par l'opérateur de services essentiels. La directive NIS ne se prononce pas sur le contenu de la notification d'incident incombant à l'opérateur de services essentiels. La directive laisse finalement à l'opérateur de services essentiels le soin de déterminer quelles sont les informations permettant à l'autorité compétente ou au CSIRT de déterminer si l'incident a un impact au niveau transfrontalier.

Le RGPD est plus précis lui sur le contenu de la notification à l'autorité de protection compétente.

L'application du RGPD et de la directive NIS pourra être concomitante si un incident de sécurité concerne des données personnelles.

5. Les États vont fournir plus d'informations

Vu l'importance du sujet, les gouvernements vont délivrer plus de renseignements aux sociétés par rapport à :

- les dernières formes d'attaques informatiques et leur provenance ;
- les destinations connues des attaques informatiques.

  Les sociétés vont être directement « informées » par leur gouvernement dans le cas où leurs systèmes ont été affectés.

Ce partage d'informations permettra d'augmenter la confiance entre l'état et les sociétés en cette matière hautement stratégique.

G. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

➟ *Fiche de guidance n° 25 : Les violations de données personnelles*

Fiche de guidance n° 41
Transformation digitale

A. L'intérêt d'une approche « *data centric* » réussie

Pour la majorité des entreprises, l'heure de la transformation digitale a sonné. La transformation digitale pousse les entreprises comme les particuliers à utiliser davantage les données informatiques. Ce virage est d'autant plus complexe à négocier que le RGPD induit des changements structurants au niveau organisationnel, technique et juridique.

Le défi va être pour les entreprises performantes :

1. de profiter de l'opportunité de la mise en conformité au RGPD pour augmenter les activités et la sécurité de l'organisation ;
2. de transformer cette conformité obligatoire en un réel avantage commercial.

Il s'agit d'augmenter la confiance des clients dans les activités digitales de la société en accélérant l'adoption par celle-ci de nouveaux outils informatiques qui vont lui permettre d'économiser des coûts et de faire un bond technologique en avant.

Le RGPD impact le cycle de vie de la donnée de bout en bout. Ce qui implique de renforcer la gouvernance et de maîtriser les processus métiers et l'architecture qui la supporte.

Il conviendra donc de mettre en place une approche globale de transformation basée sur des pratiques « *data centric* ».

À terme, ces bonnes pratiques vont contribuer à l'amélioration de la gouvernance et à l'introduction d'une véritable culture de la donnée au sein de l'entreprise. Elles faciliteront la maîtrise des risques, la qualité des données, ainsi que la sécurité et le contrôle des données et elles seront une source d'optimisation des ressources, techniques mais aussi humaines, en développant leurs compétences sur le sujet.

L'approche devrait contribuer activement à la création de valeur durable pour l'entreprise :

- par une meilleure performance des traitements ;
- par une meilleure connaissance de ses données et le développement de stratégies nouvelles de valorisation ;
- par une communication client transparente et responsable, vecteur d'une relation de confiance et durable.

Alors que de nombreuses études démontrent une perte de la confiance des consommateurs dans le digital (qui va utiliser mes données ? l'utilisation accrue de bloqueurs de publicités) (on appelle ces personnes les « *reluctant sharers* »), il est important pour une société de relever cette confiance en étant transparente vis-à-vis de ses clients et en leur montrant ce qu'elle fait avec leurs données. Les « *reluctant sharers* » doutent du digital à cause de la complexité des explications données par une société afin d'avoir accès à ses services.

Il est aussi clair que la nouvelle réglementation est un rééquilibrage entre les droits des utilisateurs et les obligations des fournisseurs de services digitaux. Les sociétés qui ne répondront pas rapidement aux demandes des consommateurs seront délaissées ou même condamnées à subir des sanctions judiciaires ou régulatoires parfois suffisamment élevées que pour détruire leurs activités.

Une fois alertés qu'ils possèdent de nouveaux droits, les « *reluctant sharers* » risquent de les exercer.

Rappelons aussi un point important : le fait de développer un tel projet de mise en conformité et d'inculquer une culture « RGPD » dans l'organisation est véritablement une tâche du top management pas de l'IT, du marketing ou du département des ventes.

B. Comment acquérir de la confiance digitale ?

Il s'agit ici d'œuvrer sur trois principes qui s'entrecroisent afin que les entreprises puissent établir valablement une relation commerciale : la transparence, le contrôle et la remédiation.

Sous l'empire du RGPD, une société sera dorénavant responsable vis-à-vis de ses consommateurs pour l'utilisation, le maintien et la protection des données à caractère personnel que ceux-ci ont bien voulu lui confier. N'oublions pas que si un consommateur n'a plus confiance en une compagnie, il peut exiger que celle-ci transmette ses données personnelles à l'un de ses concurrents (et cela par l'intermédiaire d'un simple formulaire). Il pourra également demander d'effacer les données que la société possède sur lui.

Les exigences ou réponses d'un consommateur à l'égard d'une société en qui il perd de la confiance peuvent aller du retrait de la permission de lui

envoyer des courriers commerciaux jusqu'au refus de subir dorénavant des décisions automatisées.

Dès lors, toute société devra garder la confiance de ses utilisateurs dans le but de pouvoir continuer à utiliser leurs données.

Nous pouvons nous attendre à ce que les sociétés qui sont réellement RGPD conformes le fassent savoir à leurs clients laissant sur le côté celles qui ont des difficultés dans leur travail de conformité.

C. Une sécurité optimale vis-à-vis des données personnelles des clients

Les sociétés se doivent dorénavant de correctement protéger les données à caractère personnel de leurs consommateurs. Les sociétés doivent se considérer maintenant comme gardiennes temporaires de ces données. Les personnes concernées n'ont fait que permettre aux sociétés d'utiliser leurs données temporairement et pour des finalités clairement définies et connues à l'avance.

Être conforme au RGPD peut aussi permettre aux sociétés de concurrencer des sociétés qui ne doivent pas s'y conformer. En effet, il est généralement admis que le RGPD impose des standards très stricts qui sont énormément plus respectueux des clients que, par exemple, les lois américaines. Être RGPD conforme pour une société lui apportera donc un avantage concurrentiel qu'elle pourra faire valoir globalement et non pas uniquement au niveau européen.

Le cadre réglementaire peut être aussi vu comme une assurance pour les personnes qui permettent à des sociétés d'accéder et de traiter leurs données personnelles. En effet, la loi assure les clients et les prospects que le risque qu'ils prennent en partageant leurs données est reconnu. La loi leur donnera aussi un moyen d'être indemnisé dans le cas où leurs données sont perdues ou dans le cas où la société agit de manière non appropriée.

Une donnée qui n'est pas adéquatement sécurisée est une donnée qui peut mener une entreprise à devoir à son propriétaire une indemnité. Cet actif non sécurisé peut donc devenir une menace voire une dette vis-à-vis du consommateur concerné.

D. Les actions à entreprendre

Les actions à entreprendre sont multiples.

La première étape est d'entreprendre un *data audit*. Où se trouvent les données à caractère personnel dans l'organisation ? Comment celles-ci sont-elles

traitées par la société ? Est-il encore utile pour l'entreprise de procéder à ce traitement ? Si tel n'est pas le cas, l'entreprise devrait plutôt considérer le fait d'effacer ces données et d'arrêter les traitements qui les utilisent.

Si une société estime qu'il est toujours nécessaire pour ses activités de posséder tel type de données, nous lui conseillons de vérifier si la base juridique pour les traitements choisie à l'époque est toujours valable. Dans le cas où l'entreprise a sous-traité les traitements, elle devra vérifier la conformité au RGPD de ses sous-traitants également. Il s'agira plus que sûrement de modifier les contrats qui lient la société avec eux.

N'oublions pas non plus que le RGPD requière que le responsable du traitement ne collecte que les données nécessaires aux traitements envisagés. Il s'agit aussi d'effacer les données dès que ces données ne sont plus nécessaires (*data minimisation*). Dans le cas où le responsable du traitement est la victime d'une violation de données personnelles (*data breach*), les amendes seront plus élevées si la violation a visé des données qui ne devaient plus être gardées.

Une société réellement innovatrice positionnera ses services comme utilisant ou exigeant très peu de données personnelles, spécialement si les services doivent utiliser des données considérées comme sensibles/spéciales au sens du RGPD.

Il s'agit aussi de faire attention aux logiciels dits gratuits. Ils sont souvent plus sensibles aux violations de données à caractère personnel voire demandent le plus souvent accès à l'ensemble de la banque de données clients du responsable.

Nous conseillons également aux responsables et aux sous-traitants de posséder des outils leur permettant de détecter des violations des données à caractère personnel et de les notifier à l'autorité de contrôle de données personnelles et/ou à leurs consommateurs.

Il ne s'agit peut-être pas notifier à l'autorité de contrôle de données personnelles une faille mineure. Mais si celle-ci venait à devenir récurrente, les choses pourraient évoluer. De plus, suite à une notification à l'autorité de contrôle de données personnelles, l'entreprise pourrait être obligée par celle-ci de devoir aussi notifier la violation à ses consommateurs.

Les activités devront être configurées pour être « *privacy compliant* » dès le début.

Écrire une clause vie privée complète et compréhensible pour le commun des mortels est aussi indispensable. Pas de jargon scientifique. Le responsable du traitement devra y être transparent sur les catégories de données qu'il collecte/s'apprête à collecter, sur finalités envisagées, qui va avoir accès aux données, où seront-elles stockées, pendant combien de temps, quels sont les droits des consommateurs vis-à-vis de leurs données, sur les possibles transferts de ces données hors de l'UE, etc.

Il s'agit aussi d'apprendre à chacun des employés de la société la correcte attitude vis-à-vis des données personnelles dans le but de diminuer le risque de responsabilité et, parallèlement, d'augmenter la valeur de ses actifs.

Les sociétés pourraient ou devront engager un DPD qui gèrera les problématiques *privacy* de la société.

E. Résultat

Modifier l'attitude d'une entreprise en matière de protection des données personnelles va lui permettre d'être encore plus proche de ses clients et de mieux cerner leurs doutes et soucis sur les traitements de leurs données personnelles. Si la société parvient à gérer convenablement cette relation de confiance, ses clients vont rester ses clients. Il se pourrait même qu'ils recommandent une telle société auprès de leurs connaissances.

Ce travail va, finalement, apporter un réel avantage compétitif aux sociétés qui s'y seront investies.

Fiche de guidance n° 42
Le *cloud computing* et le RGPD

A. Introduction

Les sociétés font de plus en plus appel au « *cloud computing* » (à l'infonuagique/infonuage, comme disent nos voisins français). Par exemple, pour héberger leurs nouvelles données. Et cette création de données est de plus en plus importante ! D'où l'intérêt de disposer de ressources presque illimitées et qui s'adaptent aux besoins et activités des entreprises.

Les activités des fournisseurs de services dans les nuages doivent aussi être conformes au RGPD. Les contrats avec de tels fournisseurs doivent être conformes au RGPD et prévoir entre autres la portabilité des données et le droit à l'effacement.

Toutefois, il est vrai qu'avec des données stockées dans les nuages, il n'est pas évident de déterminer où elles se trouvent exactement, qui y a accès et comment elles sont protégées.

B. Différentes sortes de *cloud computing*

Rappelons qu'il y a différentes catégories de services dans le cloud, dont principalement :

1. le *Infrastructure as a Service* (IaaS) (OVH, Azure de Microsoft, Bluemix d'IBM) ;
2. le *Platform as a Service* (PaaS) (Azure de Microsoft, Salesforce, Google Engine App, Amazon) ;
3. le *Software as a Service* (SaaS) (Dropbox, Gmail, Google Forms).

Au plus une entreprise stocke ses données et ses applications à l'extérieur de ses locaux, au plus, elle risque d'en perdre le contrôle.

La société devra, au cas par cas, analyser la sécurité du service proposé en posant les questions nécessaires et en prenant les mesures appropriées qui en découlent.

C. Marche à suivre

Il s'agit, dans un premier temps, pour la société d'analyser, en interne, ses besoins en de tels services et sélectionner le service qui répond à ses besoins (stockage ? archivage ? applicatifs ?). C'est à ce moment-là, voire en même temps que le fournisseur a été sélectionné, qu'il faut analyser les mesures de sécurité qu'il met en place.

Beaucoup d'entreprises et d'organisations (surtout les universités et les établissements d'enseignement) refusent de stocker ailleurs que chez eux leurs données. Hors de question pour eux de perdre leur indépendance numérique et d'externaliser l'hébergement des données produites, surtout si ce sont des données particulièrement sensibles. Parfois même, la loi leur interdit de stocker leurs données ailleurs que chez eux. Une solution intermédiaire est alors de mutualiser avec une autre entreprise ou entité active dans le même secteur les frais d'hébergement dans un endroit qui reste alors sous leur contrôle.

Car il s'agit avant tout de garder la maîtrise sur ses données.

Quoi qu'il en soit, qu'il s'agisse d'un stockage des données dans le cloud ou dans des *data centers* internes, les obligations légales pour les établissements restent les mêmes. En effet, l'employeur est responsable de la sécurité des données personnelles de son entreprise, y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique.

Une des questions fondamentales est de savoir qui a accès aux données stockées chez le fournisseur externe et où sont-elles stockées/hébergées (dans quel pays ?). Les mesures de sécurité suivantes devraient d'office être proposées et implémentées par le fournisseur choisi en tant que mesures pour contrer toute cyber attaque :

1. l'authentification par deux facteurs (« *two-factor authentication* »).

   Celle-ci permet d'assurer la sécurité d'accès aux données. Les personnes autorisées à accéder aux données devront s'authentifier grâce à quelque chose qu'ils ont (un téléphone par exemple) , quelque chose qu'ils sont (leur empreinte digitale par exemple) et/ou quelque chose qu'ils savent (un code ou un mot de passe) ;

2. le chiffrement (« e*ncryption* »).

   Il rend les données illisibles et dès lors inutilisables aux personnes qui y ont accédées de manière illégitime ;

3. la gestion des clefs de déchiffrement (« *key management* »).

Cette gestion permet l'accès aux clefs de déchiffrement uniquement aux personnes qui peuvent avoir accès aux données. Il arrive parfois aussi que les clefs de déchiffrement soient gardées sur des disques externes pour empêcher leur vol à distance ;

4. restauration rapide des données.

   La possibilité de récupérer rapidement les données en cas d'incident (incendie, attaque informatique, etc.) est très importante ;

5. les fournisseurs de services cloud doivent apporter des garanties suffisantes que le service est conforme aux exigences techniques et organisationnelles du RGPD ;

6. les contrats de service entre le responsable du traitement et le sous-traitant doivent interdire le recours à d'autres sous-traitants sans le consentement préalable du responsable du traitement ;

7. à l'expiration du contrat de service, toutes les données doivent être supprimées du cloud et le sous-traitant doit apporter les preuves suffisantes que c'est bien le cas ;

8. les responsables du traitement ont l'obligation de rendre compte de tout incident de fuite de données à l'autorité de contrôle des données personnelles.

   Lorsque le RGPD entrera en application (en mai 2018), les sociétés qui auront été la victime de violations de données à caractère personnel (« *data breach* ») devront le notifier aux autorités de protection de données personnelles et parfois même aux personnes concernées. Ces sociétés ne pourront plus cacher ces attaques et violations. Si les sociétés n'auront pas mis en place d'ici là les mesures de sécurité adéquates, elles risquent d'énormes amendes. C'est pourquoi, il est indispensable que le contrat avec le sous-traitant prévoie les mesures nécessaires à ce sujet et qu'il a l'obligation de prévenir le responsable du traitement dans un délai très court (24h ?) dès qu'il a connaissance de la violation.

Toutefois, la négociation en matière de contrat cloud est très difficile.

En effet, ces contrats sont souvent considérés comme des contrats d'adhésion (des contrats-type « à prendre ou à laisser ») sur lesquels portent pourtant des contraintes réglementaires en matière de protection des données personnelles de plus en plus fortes.

Une entreprise qui s'apprête à confier tout ou partie de ses données à un prestataire de cloud dispose donc d'une marge de négociation contractuelle nulle ou très réduite.

La situation évolue pourtant grâce à la pression concurrentielle. Les services de cloud font du respect de normes telles que les normes ISO 27001 et 27018 dédiées à la sécurisation des données un argument commercial.

Mais c'est surtout le RGPD, directement applicable dans tous les États membres le 25 mai 2018, qui va impacter la matière et modifier en profondeur les règles applicables à l'environnement digital des entreprises.

Le RGPD introduit ici surtout une coresponsabilité de la sanction financière entre les parties sur laquelle peut jouer le responsable du traitement. Or, rappelons que les sanctions financières encourues peuvent aller jusqu'à 4 % de son chiffre d'affaires mondial ou 20 millions d'euros.

Les fournisseurs de cloud américains d'eux-mêmes modifient leurs pratiques. Ainsi, il n'est pas rare de les voir offrir aux entreprises européennes :

1. la certitude de la localisation de leurs données.

   Le fournisseur certifie contractuellement que les données de l'ensemble de ses services restent en Europe ;

2. un contrôle sur leurs données.

   Chaque entreprise est responsable de la protection de ses données. Ceci implique de savoir qui y a accès et quand. Le fournisseur cloud déclare déployer des contrôles pour s'assurer que l'accès au contenu du client (y compris les données personnelles du client et les données personnelles spécifiques) est limité et contrôlé/réalisé uniquement par des employés basés dans l'Union européenne. Le fournisseur assure aussi que ces employés examineront au cas par cas et approuveront (réaliseront ?) tous les changements apportés par des employés du fournisseur qui ne sont pas basés dans l'Union européenne qui pourraient affecter les données de clients européens. Le fournisseur peut aussi ajouter que ce seront aux clients européens à examiner et à approuver toutes les demandes d'accès à leur contenu non-UE si une instance de contrôle nécessite le support ou l'accès d'un employé basé en dehors de l'Union européenne. Les journaux qui tracent les accès à leurs données peuvent aussi être mis à la disposition du client ;

3. capacités de chiffrement avancées.

   Le fournisseur déploie souvent des fonctionnalités très avancées permettant à ses clients de chiffrer leurs données – au repos et en transit – avec leurs propres clés principales. Rappelons que le chiffrement des données permet de stocker les données dans le cloud et de les protéger contre le vol et les compromissions. Par l'intermédiaire de cette possibilité, les clés resteront en possession du client afin que les données soient protégées des fournisseurs de services cloud ainsi que des autres utilisateurs.

Une entreprise en position de force pourra aussi tenter d'inclure dans son contrat une clause d'audit. Toutefois, cette clause risque d'être difficile à obtenir et sera souvent limitée à une visite annuelle du *datacenter* à date fixe. Il est aussi conseillé de renforcer les pénalités financières en cas de manquement aux engagements « qualité » (SLA).

D. Analyse de quelques points en particulier

L'onde de choc du RGPD aura un impact majeur sur tous les prestataires de stockage de données mais aussi sur les acteurs en charge de l'archivage électronique.

1. Archivage

En effet, les documents électroniques archivés (contrats, bulletins de souscription, documents RH, etc.) peuvent contenir des données à caractère personnel. Lorsque l'archivage des documents d'une organisation (le responsable du traitement au sens de la réglementation) est confié à un prestataire d'archivage (le sous-traitant), le responsable du fichier/traitement a la responsabilité de s'assurer que son prestataire présente des garanties suffisantes en matière de sécurité et de confidentialité des données qui lui sont confiées. Celui-ci devra donc fournir au responsable du traitement les éléments lui permettant, qu'il s'agisse d'une entreprise, d'une entité ou d'une collectivité de faire face aux différentes contraintes et formalités imposées par le règlement.

2. Cloud

La question à se poser est celle-ci : les services dans le cloud le sont-ils conformément au RGPD ?

a. *Responsable de traitement. Qui ?*

Ce sera la plupart du temps la société qui fait appel au service cloud qui définira les finalités (le quoi du traitement) et les moyens (le comment, à savoir l'utilisation du service en question).

Ce sera donc bien à la société qui fait appel au service dans le cloud de s'assurer du respect général de la réglementation.

b. *Le respect des principes édictés par le RGPD*

La société en question devra *ab initio* respecter les principes suivants :

- transparence ;
- données collectées pour des finalités déterminées, explicites et légitimes et sans utilisation ultérieure d'une manière incompatible avec ces finalités ;

- minimisation des données ;
- durée de conservation limitée ;
- sécurité ;
- *accountability, Privacy by design* et *Privacy by default*.

Analyse de chacun de ces principes

Transparence

Cela implique entre autres une information claire des personnes concernées, telle qu'imposée par l'article 13 du RGPD.

L'article 13.1.f du RGPD de cet article impose d'informer de tout transfert de données hors UE et des garanties appropriées.

Il faudra que la société utilisant le service infonuagique se renseigne sur le lieu de stockage des données recueillies grâce au service SaaS (UE, USA, …). Si les données sont stockées aux USA, il faudra que la société soit sûre que la société proposant le cloud ait adhéré au *Privacy Shield*.

Données collectées pour des finalités déterminées, explicites et légitimes et sans utilisation ultérieure d'une manière incompatible avec ces finalités

La société qui utilise le service dans le cloud ne pourra utiliser les données récoltées de ses clients que pour les finalités énoncées. À charge aussi pour elle de s'assurer que les données ne soient pas utilisées ultérieurement par le fournisseur du service dans le cloud (car ces données peuvent avoir de la valeur pour elle). Il faudra bien lire les conditions générales d'utilisation du service en question et ses clauses additionnelles qui sont particulièrement instructives sur les données recueillies et leur usage pour le savoir. Il serait préférable de bien spécifier que ce ne sont que les données qui sont transférées dans le cloud et que le responsable du traitement en garde la propriété.

Minimisation des données

Ce sera à la société qui va utiliser le service externe à définir les données qu'elle entend utiliser via ledit service.

Il reste à savoir si la société proposant le service ne va pas elle recueillir d'autres données telles que l'adresse IP ou si elle ne va pas associer ces données à d'autres éléments qu'elle pourrait posséder déjà.

Durée de conservation limitée

Une fois que la société ayant utilisé le service dans le cloud a traité les données recueillies grâce au service, elle devra logiquement supprimer les

données à caractère personnel recueillies. Cette suppression devrait être réalisée selon un plan de suppression des données préétabli.

Toutefois, la société devra s'assurer que la société qui a proposé le service dans le cloud a bien aussi supprimé les données en question en ce compris dans ses back-ups de sauvegarde qui peuvent se retrouver n'importe où.

Sécurité

La société qui recueille les données doit s'assurer que les données soient bien sécurisées chez elle. Il faudra aussi qu'elle s'assure de la sécurité de la société qui propose le service dans le cloud.

Accountability, Privacy by design *et* Privacy by default

Au-delà des principes de base listés par l'article 5 du RGPD et qui existent déjà bien souvent dans la réglementation actuelle, la société qui utilise le service dans le cloud devra aussi respecter les principes dit de responsabilité (*Accountability*, article 24) et de Protection des données dès la conception et Protection des données par défaut (*Privacy by design* et *Privacy by default*, article 25).

De plus, elle devra réaliser une analyse de l'article 28 du RGPD qui liste les conditions d'une « bonne » sous-traitance.

En effet, la société qui propose le service dans le cloud est un sous-traitant (la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement).

Le responsable de traitement doit donc s'interroger (en analyse préalable = *Accountability* et *Privacy by design*) :

- la société qui propose le service dans le cloud met-elle en œuvre en œuvre des « mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée » ? Quelles sont les conséquences en matière de sécurité et de protection des données personnelles hébergées dans le cloud des technologies utilisées par le fournisseur dudit service ?
- les conditions d'utilisation et autres politiques de cette société sont-elles conformes à l'article 28.3 du RGPD ?

  Le contrat (e.a.) devra mentionner comment le sous-traitant devra aider le responsable du traitement à répondre aux demandes des personnes concernées. Par exemple, le contrat devrait prévoir le format des données que le sous-traitant devrait utiliser dans le cas où le responsable du traitement est saisi d'une demande de portabilité ;
- les conditions de notification d'une violation de donnée en 72 heures sont-elles possibles ?

Si une violation de données personnelles devait arriver chez le fournisseur du service dans le cloud, le responsable de traitement a également 72h pour notifier la faille à l'autorité de contrôle dont il dépend. Les règles ne changent pas. Dès lors, il est primordial que le responsable du traitement soit assuré que la société qui propose le service dans le cloud l'informera à temps (et de manière suffisamment complète) afin qu'il puisse remplir ses obligations.

E. Attention au « *vendor lock-in* »

Le choix d'utiliser une solution cloud est souvent dicté par la volonté de réduire les coûts. Au lieu d'avoir dix informaticiens en interne, la société en externalise la moitié (souvent à très moindre coût au vu de la baisse constante des solutions cloud, spécialement celles relatives au stockage des données) pour ne garder qu'une partie de l'équipe sur son *payroll*.

Attention toutefois à la problématique de la sortie du service cloud choisi. C'est ce que l'on appelle le « *vendor lock-in* ». La société va d'abord confier un service ou une application à la société externe pour ensuite, attirer par son bon langage marketing, beaucoup plus.

Si, à un moment donné, la société désire stopper ses activités dans le cloud, les diminuer ou les transférer, cela risque d'être très difficile. Et parfois aussi très cher. Souvent, il faudra reconstruire ce que l'on avait voulu éviter.

En ce qui concerne les données à caractère personnel, la société devra s'assurer d'avoir le temps de récupérer ses données. Par exemple, Microsoft 365 ne nous laisse que 90 jours pour rapatrier nos données dans le cas où on arrête de l'utiliser.

Il faudra aussi s'assurer que l'application ou le service (interne ou externe) qui va récupérer les données puisse les lire et que les données aient effectivement été effacées dans les servers du fournisseur de la solution cloud.

Il est fortement conseillé d'avoir une politique de sortie dès que l'on choisit d'aller vers le cloud.

F. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

➠ *Fiche de guidance n° 9 : La protection de données personnelles*

Fiche de guidance n° 43
Le « *legal assessment* »

A. Introduction

Tout projet de transformation doit commencer par une évaluation de la situation actuelle de l'entreprise : où en est-elle par rapport aux droits et obligations qui existent déjà aujourd'hui ? Où en est-elle par rapport aux droits et exigences du RGPD ?

Afin d'analyser le travail de conformité à réaliser, chaque entreprise doit se poser un certain nombre de questions. Ces questions doivent permettre à la société d'évaluer sa situation et de déterminer le travail qu'il reste encore à réaliser pour être en conformité avec le RGPD. C'est ce que l'on appelle, effectuer un « *Legal Assessment* ».

B. Exemples de *Legal Assessment*

Voici quelques questions qui pourraient être incluses dans un bon « *Legal Assessment* » :

1. Votre *senior management* est-il au courant des diverses implications du RGPD pour l'ensemble de la société ? Supporte-t-il le travail de mise en conformité ? Participe-t-il aux séances d'information (« *awareness* ») ?

   OK : ❑

   NOK : ❑

2. Avez-vous déjà nommé un DPD ? Dispose-t-il des ressources (informatiques et opérationnelles) adéquates pour faire face aux nouvelles exigences du RGPD ?

OK : ❑

NOK : ❑

3. L'ensemble du personnel a-t-il suivi une quelconque formation autour du RGPD ? Réalisez-vous un *reporting* adéquat du suivi du personnel par rapport à cette formation ? Visez-vous le 100 % ? Un autre résultat ?

OK : ❑

NOK : ❑

4. Une donnée à caractère personnel est une donnée relative à une personne identifiée ou identifiable. Traitez-vous des données à caractère personnel ?

OK : ❑

NOK : ❑

5. Certaines catégories de données sont plus protégées que d'autres (les données médicales, génétiques, judiciaires). Traitez-vous ces catégories de données ?

OK : ❑

NOK : ❑

6. Savez-vous où se trouvent vos données à caractère personnel ? Avez-vous nommé un « *data owner* » par catégorie de données ? Avez-vous nommé un *Chief Data Officer* ?

OK : ❑

NOK : ❑

7. Certaines de vos données sont-elles situées/transférées hors de l'UE ? Avez-vous analysé l'ensemble de ces transferts ?

OK : ❑

NOK : ❑

8. Pouvez-vous identifier la base juridique relative à chacun de vos traitements ?

OK : ❑

NOK : ❑

9. Avez-vous ou pouvez-vous cartographier l'ensemble des traitements que votre société réalise ceci afin de mettre en place un registre des traitements ? Disposez-vous déjà d'un outil adéquat ?

OK : ❑

NOK : ❑

10. Avez-vous une clause vie privée (un « *Privacy Statement* ») ?

OK : ❑

NOK : ❑

11. Avez-vous déjà en place des outils informatiques afin de pouvoir dans le délai requis et adéquatement répondre aux droits des personnes concernées ?

OK : ❑

NOK : ❑

12. Le RGPD vous impose de sécuriser adéquatement les données que vous traitez. Pouvez-vous décrire les mesures de sécurité que vous avez aujourd'hui implémentées autour de ces données ?

OK : ❑

NOK : ❑

13. Avez-vous récemment revu vos contrats avec vos sous-traitants ?

OK : ❑

NOK : ❑

14. Vos données sont-elles adéquatement classées et gérées (« *data classification* ») ?

OK : ❑

NOK : ❑

15. Connaissez-vous la période pendant laquelle vous pouvez garder de manière non anonyme chacune de vos données ?

OK : ❑

NOK : ❑

16. Avez-vous déjà en place une procédure afin de réaliser quand cela est nécessaire une analyse d'impact relative à la protection des données (AIPD) ?

OK : ❑

NOK : ❑

17. Avez-vous déjà en place une procédure en cas de violation de données à caractère personnel ?

OK : ❑

NOK : ❑

18. Êtes-vous préparé à implémenter les règles « *Privacy by Design* » et de « *Privacy by Default* » du RGPD ?

OK : ❑

NOK : ❑

19. Avez-vous de la documentation afin de bien pouvoir expliquer chacune de vos précédentes réponses ?

OK : ❑

NOK : ❑

C. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

➠ *Annexe 2 – Bonus 2 : Aperçu des mesures à entreprendre pour être conforme au RGPD*

Fiche de guidance n° 44
le RGPD et le (direct) marketing

A. Introduction

Le RGPD ne modifie pas énormément les règles anciennes en ce qui concerne le marketing direct (ou la prospection) électronique. En effet, la réalisation d'actions de marketing direct électronique dépend des règles de l'*ePrivacy* (directive de 2002 modifiée en 2009 et dont les règles sont pour l'instant en cours de modification).

N'oublions toutefois pas que le RGPD oblige aussi les entreprises à plus de protection avec une meilleure sécurisation des données, la mise en place de procédures en cas de vol ou perte de données, mais également plus de transparence.

Les actions de marketing direct sont des actions de promotion personnalisées à opposer à des actions de promotion générales comme la mise en place de bannières électroniques ou le placement d'affiches dans des abribus. Le marketing direct est donc un concept très large. Il ne s'agit pas uniquement des actions commerciales d'entreprises vers leurs clients, mais également des prises de contacts avec des prospects, donc des clients potentiels.

Pour pouvoir réaliser une action de marketing direct électronique, une société a besoin :

1. des coordonnées de contact électronique (email, SMS, fax) ;
2. de l'accord de la personne pour recevoir le message électronique.

La société a en effet besoin de l'accord de la personne avant même de lui envoyer le message publicitaire électronique. C'est ce que l'on appelle couramment l'« *opt-in privacy* ».

On l'oppose à l' « *opt-out papier* ». Une société peut envoyer un courrier publicitaire papier même personnalisé à une personne sans son autorisation préalable. Toutefois, l'entreprise devra arrêter de contacter ainsi la personne dans le cas où la personne s'y est opposé (par exemple via son inscription en Belgique sur la liste Robinson).

De même, une personne peut s'inscrire sur la liste « Ne m'appelez plus » dans le but de ne plus recevoir des appels téléphoniques publicitaires. Dans ce cas, les entreprises et organisations enlèveront le numéro de téléphone et le nom de leur liste et n'appelleront plus la personne pour promouvoir leurs produits et services.

Dans la réalisation de son action de marketing direct, la société va très souvent tenter de cibler au mieux les destinataires de son emailing publicitaire (ses « *targets* »). Ceci dans le but de le rendre au maximum effectif. En effet, au plus un message électronique est personnalisé à la situation des « *targets* », au mieux il pourrait mener à la concrétisation de ventes. On appelle cela la publicité ciblée.

La société va traiter les données de ses clients qu'elle possède dans son CRM (« *Customer relationship management* », un logiciel chargé de gérer la relation client) afin d'en retirer les meilleures listes possibles en fonction des messages qu'elle veut envoyer.

Entrent ici en jeu les travaux des *data analysts* et des *data scientists* (parfois aussi écrit en un mot). Ces spécialistes du chiffre et des modèles mathématiques ainsi que du big data vont, à l'aide de procédures mathématiques ou statistiques, triturer les données de la clientèle ainsi que les flux de ces données (géolocalisation, *clickstream*, ou objets connectés – ce qui est beaucoup plus intéressant) pour en faire ressortir des listes optimales en fonction des messages publicitaires préparés par l'équipe marketing de la société.

On s'aperçoit qu'au plus la société possède de données sur ses clients (nom, adresse, adresse email des internautes, grandeur du ménage, classe de revenus, pouvoir d'achat, habitudes des abonnés mais aussi leur comportement en ligne = quelles pages du site, tel internaute visite le plus souvent, etc.), au plus les modèles pourront être efficaces. C'est pourquoi aussi les sociétés acquièrent de plus en plus d'autres sociétés uniquement dans le but de récupérer comme trésor de guerre les données que les sociétés acquises possèdent dans leur CRM.

Les *data analysts* et des *data scientists* travaillent généralement sous la responsabilité du *Chief Data Officer* (CDO) de la société. Il s'agit du véritable directeur des données possédées par une société. Son rôle principal est de faciliter l'accès aux données stockées par une entreprise. Il doit s'assurer de la fiabilité de celles-ci pour permettre leur bonne exploitation et analyse. Tout ceci afin de permettre à la Direction de prendre les meilleures décisions.

Un des rôles clé du *Chief Data Officer* est de pouvoir choisir, parmi la profusion des données, celles qui seront les plus utiles pour son entreprise et d'agréger toutes les datas internes et externes afin de rendre les analyses pertinentes. Le *Chief Data Officer* va aider le DPD dans la mise en conformité de leur entreprise au RGPD en responsabilisant les acteurs traitant les données.

B. Les règles du RGPD en la matière

1. Le consentement

Beaucoup d'entreprises se demandent si elles ne doivent pas redemander le consentement à leurs clients et prospects avant de leur envoyer à nouveau des messages publicitaires après le 25 mai 2018.

La réponse à cette épineuse question n'est pas évidente.

Il faut savoir que le RGPD ne contient aucune règle de transition, autre que la période d'« implémentation » de deux ans entre 2016 et 2018.

À partir du 25 mai 2018, toutes les exigences du RGPD devront avoir été comprises et implémentées par les entreprises.

Une entreprise ne peut effectuer un traitement sur des données à caractère personnel que sur la base d'une des six bases juridiques de l'article 6 du RGPD.

Si la société concevait son marketing direct sur la base du consentement des personnes concernées et qu'elle entend continuer à faire de même, il lui faudra vérifier si le consentement qu'elle avait obtenu est équivalent au consentement version RGPD.

Nous craignons que, dans la plupart des cas, les sociétés doivent se rendre compte que le consentement qu'elles avaient obtenu n'est nullement le même vu les conditions nouvelles très strictes imposées à celui-ci par l'article 7 du RGPD.

Dans un tel cas de figure, les sociétés n'auront d'autre choix que de redemander le consentement à leurs clients/prospects et cette fois-ci en respectant les exigences du nouveau Règlement.

Le consentement n'est qu'une des six bases juridiques de tout traitement.

La société pourrait baser ses traitements relatifs à son marketing direct sur ses intérêts légitimes. En effet, le considérant 47 du RGPD lui-même précise que tel peut être le cas. Rappelons que, dans ce cas, le responsable devra effectuer une analyse des intérêts en présence et archiver sa décision.

La réglementation en matière de marketing électronique est aussi gouvernée par la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques modifiée en 2009).

Suite à cette directive :

1. les entreprises ne peuvent envoyer des mailings électroniques qu'avec l'accord préalable des destinataires de ces e-mailings ;
2. il est possible pour les sociétés d'envoyer du marketing électronique à leurs clients pour des produits similaires à ceux pour lesquels les personnes sont devenues clientes de la société. C'est ce que l'on appelle

l'« exception produits ou services similaires », exception au fait de pouvoir agir sans disposer du consentement préalable des personnes concernées. Par exemple, une compagnie d'assurances peut envoyer un email de direct marketing relatif à une campagne assurance « auto » à ses clients en assurance « habitation » sans disposer au préalable de leur consentement. Les deux produits peuvent, en effet, être considérés comme similaires ;

3. chaque emailing publicitaire doit contenir une procédure facile pour le destinataire de l'email pour se désinscrire, pour refuser de recevoir dans le futur d'autres emails publicitaires de la même société. À charge évidemment pour la société de gérer en interne correctement les oppositions (les *opt-out* comme on dit) des destinataires des emails.

   Puisqu'il est facile de collecter des adresses électroniques et d'envoyer des emails publicitaires, il doit être facile et efficace pour la personne de refuser d'en recevoir encore dans le futur.

Dès lors, si la société ne peut/veut justifier ses campagnes de marketing direct sur la base de ses intérêts légitimes, ne dispose pas des consentements adéquats version RGPD et veut réaliser des campagnes de marketing qui ne tombent pas sous l'exception « produits ou services similaires », elle devra obligatoirement obtenir le consentement RGPD des personnes concernées.

2. La transparence

Le RGPD prévoit le principe de traitement loyal et transparent. Celui-ci implique que la personne concernée soit informée de l'existence de toute opération de traitement et de ses finalités au moment de la collecte de ses données à caractère personnel ainsi que de l'existence d'un profilage et des conséquences de celui-ci.

Le considérant 71 du RGPD définit le profilage comme une opération qui

> « consiste en toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements, dès lors qu'il produit des effets juridiques concernant la personne en question ou qu'il l'affecte de façon similaire de manière significative ».

L'article 21 du RGPD prévoit ici des règles particulières.

Cet article, intitulé « droit d'opposition » précise en effet que :

1. la personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6.1.e (traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de

l'exercice de l'autorité publique) ou 6.1.f (le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers), y compris un profilage fondé sur ces dispositions.

Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice ;

2. lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection ;
3. lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données à caractère personnel ne sont plus du tout traitées à ces fins ;
4. au plus tard au moment de la première communication avec la personne concernée, les droits visés aux points 1 et 2 sont explicitement portés à l'attention de la personne concernée et sont présentés clairement et séparément de toute autre information ;
5. dans le cadre de l'utilisation de services de la société de l'information, et nonobstant la directive 2002/58/CE, la personne concernée peut exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.

En résumé, une société, au moment où elle collecte les données personnelles, devra (si elle entend le faire par après bien sûr) (mais c'est presque devenu monnaie courante dans toutes les sociétés réalisant du marketing direct pour les raisons évoquées plus haut) informer les personnes concernées qu'elle va traiter leurs données à des fins de marketing direct en ce compris en les profilant. Les personnes concernées pourront à tout moment s'opposer au marketing direct et à leur profilage et ce au moyen si possible de procédés simple d'utilisation. La règles étant que puisqu'il est si facile de collecter des données à caractère personnel, il devrait être tout aussi facile pour les personnes concernées de s'opposer au marketing direct et au profilage.

La société devra informer de ces possibilités les personnes concernées par l'intermédiaire de sa Charte Vie Privée qui doit être aisément consultable sur son site web.

Dans sa Charte Vie Privée, la société devra indiquer qu'elle a l'intention de traiter les données des personnes concernées à des fins de prospection. Elle devra indiquer la base juridique d'un tel traitement. Dans le cas (le plus probable) où cette base juridique sont les intérêts légitimes de la société prévalant sur les intérêts ou les libertés et droits fondamentaux de la personne concernée,

la société doit indiquer « les intérêts légitimes poursuivis » par le responsable du traitement (ou par un tiers).

Comment atteindre le juste équilibre entre expérience client exceptionnelle et personnalisée et sécurité maximale des données collectées ?

L'entreprise ne voudra pas sacrifier l'un pour l'autre.

Il lui faudra expliquer à ses clients les bienfaits d'une expérience personnalisée et les persuader qu'elle a la capacité à gérer correctement leurs données. L'entreprise sera alors à même de les récompenser avec des offres ciblées et des remises alignées sur leur comportement d'achat.

L'entreprise devra aussi faire preuve de transparence quant à sa politique de gestion des données de ses clients et leur faire comprendre l'intérêt pour eux de bien vouloir partager leurs informations personnelles.

Les clients mis devant le fait accompli seront probablement plus sur la défensive et moins coopératifs que s'ils sont impliqués dès le départ dans une démarche globale qui vise à mieux les servir.

C. Les règles de l'*ePrivacy*

Le RGPD n'est pas le seul texte à régir la matière de la protection des données personnelles. L'Europe dispose aussi d'une directive votée en 2002 (et modifiée en 2009) en matière de communications électroniques.

Ces règles sont appelées à évoluer dans un futur proche. En effet, la Commission européenne a déposé en janvier 2017 une proposition de Règlement pour la *ePrivacy*. Le texte est toujours en discussion au Parlement européen.

La directive de 2002 concerne aussi les cookies électroniques. Les cookies sont des petits logiciels informatiques qui sont déposés sur votre ordinateur lorsque vous visitez un site web.

Ces cookies sont parfois très utiles. Ils peuvent retenir la langue de votre navigation ou votre panier d'achat lorsque vous achetez en ligne et que le site de vente est composé de plusieurs pages web. Les cookies peuvent aussi servir à vous tracer (« le *tracking* ») sur internet et à vous proposer de la publicité ciblée pour un produit A sur un site web X alors que vous avez fait une recherche sur un moteur de recherche pour le produit A deux jours auparavant.

Les règles actuelles prévoient que vous devez être informés que le site web que vous vous apprêtez à visiter utilise des cookies. C'est l'objet de la bannière électronique cookies que vous voyez apparaître lorsque vous visitez pour la première fois un site web. Le site n'est pas obligé de vous permettre de refuser ses cookies mais il doit vous renvoyer vers sa politique en la matière.

Sachez que vous pouvez gérer les cookies que votre ordinateur peut recevoir via les options de votre navigateur web (les refuser en bloc, en accepter certains et effacer ceux que votre ordinateur a déjà reçu).

D. Les autres Fiches de guidance de l'ouvrage en rapport avec le sujet

- *Fiche de guidance n° 6 : Le consentement*
- *Fiche de guidance n° 35 : Le big data et le RGPD*
- *Fiche de guidance n° 37 : ePrivacy*

Fiche de guidance n° 45
La blockchain face au RGPD

A. Introduction (sommaire)

La blockchain est une nouvelle technologie amenée à transformer notre manière de travailler. Une blockchain crée des banques de données décentralisées. Les participants à une blockchain (ou à une « *Distributed Ledger Technology* » – DLT) voient chacun la même banque de données qui est actualisée en temps réel.

La première blockchain est apparue avec les bitcoins en 2007-2008. Depuis lors, beaucoup d'autres ont émergé. Cette nouvelle technologie révolutionnaire va modifier énormément notre vision et notre façon de travailler comme internet l'a fait depuis son arrivée.

Les blockchains reposent sur plusieurs technologies existantes (comme la cryptographie asymétrique ou la signature électronique) mais dont la combinaison n'a été rendue seulement possible qu'aujourd'hui grâce à la puissance de calcul exponentielle de nos ordinateurs actuels.

Il y a plusieurs sortes de blockchain :

1. des blockchains liées à l'échange de crypto-monnaies comme la blockchain Bitcoin ;
2. des blockchains qui permettent de réaliser des transactions liées à des « *smart contracts* » ;
3. des blockchain où tous les participants ont connaissance de l'ensemble de la banque de données qui y est liée (on appelle ces blockchain, des blockchain publiques ou « *permissionless* » en anglais) ;
4. des blockchains où, inversement, uniquement certains participants peuvent voir la banque de données (les blockchain privées ou « *permissioned* » en anglais). Ces blockchains sont gérées par une organisation ou un centralisateur.

Des « *smart contracts* » sont des contrats informatisés immuables. Il s'agit de contrats fondés sur le fait que SI un évènement se produit ALORS telle transaction doit automatiquement se réaliser (« …*if*...*then*… »).

Par exemple, il existe sur le marché des contrats d'assurance blockchain qui indemnisent automatiquement et sans intervention de la compagnie d'assurances le preneur d'assurance dans le cas où son vol a un certain retard. La vérification du retard effectif est vérifiée auprès d'opérateurs et de services de confiance externes (les oracles).

Les blockchains comme la blockchain Bitcoin peuvent être vues comme des suites de blocs. Chaque bloc contient un ensemble de transactions. Les blocs sont analysés et approuvés par des mineurs (des « *miners* ») à intervalle régulier. Les « *miners* » sont mis en compétition. D'ailleurs, celui qui, le premier grâce à la puissance de calcul de son ordinateur ou de son groupe d'ordinateurs, a résolu le calcul demandé pour approuver le bloc reçoit des bitcoins comme récompense.

B. Avantages et inconvénients d'une blockchain

Un bloc à approuver contient un résumé du bloc précédent. Une fois le bloc approuvé, il est « enchaîné » à la blockchain. Il se verra adjoindre le bloc suivant et ainsi de suite. On le voit, au plus la blockchain avance dans le temps, au plus, il est difficile voire quasi impossible de modifier une transaction précédente.

Les apports principaux de la blockchain sont :

1. l'absence d'autorité centrale approuvant ou désapprouvant les transactions (à terme, les blockchain pourraient conduire à la disparition des intermédiaires en immobiliers (comme les notaires), financiers (comme les banques) ou en assurance (les courtiers)) ;
2. l'irréversibilité des transactions approuvées chronologiquement ;
3. deux transactions ne peuvent concerner la même cryptomonnaie ou dit autrement, une cryptomonnaie ne pourra jamais être dépensée deux fois au même moment par la même personne ;
4. la pseudonymisation des personnes impliquées dans les transactions.

   L'identité de ces personnes est remplacée par des identifiants informatiques. Il est possible de savoir qui se cache derrière les identifiants mais ce n'est pas facile ;
5. la transparence relative aux transactions approuvées puisque l'on peut remonter dans le temps jusqu'au début de la blockchain en question.

Les principales difficultés liées à la blockchain sont :

1. la méconnaissance du sujet par le public liée à sa nouveauté et au fait que la technologie évolue constamment. Elle n'est pas figée ;
2. l'intégration de cette nouvelle technologie dans les systèmes existants (ce que l'on appelle la « *legacy issue* » en anglais) ;
3. l'ignorance quant au fait de savoir si les blockchains pourront adéquatement ou non supporter les milliers de transaction à la minute qui se réalisent de par le monde.

   Par exemple, la blockchain Bitcoin n'approuve qu'une dizaine de transactions par délai de dix minutes. Ce n'est pas du tout comparable aux 11.000 transactions gérées par seconde par VISA ;
4. la création de standards.

   Pour l'instant, les sociétés se lancent dans des projets pilotes relatifs aux blockchains. Il est à espérer que des modèles en sortiront, que des moyens de communiquer entre les diverses blockchains seront aussi créés en même temps et que, finalement, des standards internationaux émergeront permettant de créer des blockchain efficaces et interopérables.

C. Le RGPD et les blockchains

Le RGPD renforce les droits des personnes dont les données à caractère personnel sont traitées par des sociétés. Nous l'avons vu dans les fiches précédentes, le RGPD renforce les droits en matière de consentement, de droit à l'information, de droit d'accès, de rectification et de portabilité, en matière de droit à l'oubli et de mesures de sécurité.

L'importance est particulièrement mise dans le RGPD sur la sécurité et la confidentialité des données.

Les participants peuvent déposer des données personnelles sur une blockchain. Elles peuvent aussi y déposer un « *hash* » du document. Le *hash* est une transformation du document en une suite unique de 64 caractères alphanumériques. Un document donnera toujours le même *hash*. Si nous avons un *hash* en face de nous, il nous est impossible de deviner le document original et surtout de faire le chemin inverse et de retrouver le document en question. La chance est infime d'avoir deux *hash* identiques.

Une blockchain pourrait être conçue pour stocker des données d'identification de personnes.

Les blockchain privées, contrôlées par un responsable, permettent l'application classique et entière du droit des données personnelles. Ripple, par exemple, contrôle son réseau et en assume donc la responsabilité juridique.

Les blockchains ouvertes, comme Bitcoin ou Ethereum, concentrent les principales problématiques juridiques.

Voici quelques points à avoir à l'œil dans le cas où il est décidé de déposer des données personnelles sur une blockchain publique.

Données personnelles

Une blockchain peut contenir des données personnelles au niveau de la transaction. En effet, à l'occasion d'une transaction, les utilisateurs ont la possibilité d'inscrire une faible quantité de données, comme l'empreinte numérique d'un document. Rien n'interdit que cette donnée – un identifiant, un numéro de téléphone ou un nom – se rapporte à « une personne physique identifiée ou identifiable » et entre de ce fait dans le champ d'application du RGPD.

Responsable du traitement

Une blockchain ouverte, en tant que protocole, ne peut être responsable du traitement des données qui y sont inscrites. Le RGPD définit le responsable comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

La blockchain n'est pas un service, comme peut l'être un logiciel, mais un protocole, comme le TCP/IP pour Internet ou le SMTP/IMAP pour les mails, c'est à dire un langage informatique permettant à des machines de communiquer au moyen d'applications (Chrome, Firefox ou Safari pour internet par exemple).

Aucun des acteurs de la blockchain (mineurs, développeurs, utilisateurs, …) n'est susceptible de répondre à la qualification de responsable du traitement.

Dans une architecture totalement décentralisée et ouverte, aucun acteur ne possède l'autorité ou le pouvoir susceptible de lui conférer la qualité de responsable du traitement :

1. les développeurs du code source agissent généralement sous des pseudonymes et sont désintéressés, si ce n'est bénévoles. Juridiquement, ils agissent dans le cadre d'une licence libre (« *open source* ») qui garantit la réutilisation du code ;
2. les mineurs ont un simple rôle technique de validation des transactions, sans connaissance du contenu de celles-ci. À ce titre, leur statut est comparable à celui de prestataires techniques (les fournisseurs d'accès à internet (FAI), hébergeur).

Si la technologie blockchain peut contenir des données personnelles, l'absence de responsable du traitement exclut l'application directe du RGPD. En effet, les droits consacrés par ce règlement, comme le droit à l'effacement, ne peuvent être sanctionnés directement par le protocole. En revanche, les services aux frontières de la blockchain, comme les plateformes de change, les processeurs de paiement ou les explorateurs de blockchain, devront appliquer le RGPD dans la mesure où ils sont responsables du traitement. Comme Google, qui doit faire disparaître des résultats de son moteur de recherche des données

personnelles « inappropriées, hors de propos ou qui n'apparaissent plus pertinentes », les services tiers à la blockchain devront être en mesure de faire respecter le droit à l'oubli en rendant les données inscrites sur la blockchain inaccessibles.

La pseudonymisation

Le RGPD incite les entreprises à privilégier l'utilisation de pseudonymes avant et pendant le traitement des données pour en garantir la protection.

La « pseudonymisation » consiste à s'assurer que les données sont conservées sous une forme ne permettant pas l'identification directe d'un individu sans l'aide d'informations supplémentaires.

La blockchain assure cette fonctionnalité en permettant aux utilisateurs d'utiliser des adresses publiques pseudonymisées qui ne révèlent rien en soi sur leur propriétaire.

Cependant, cela ne suffit pas à écarter la qualification de donnée personnelle. En effet, le RGPD précise qu'il convient « de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement » pour considérer une donnée comme personnelle.

Il existe des outils informatiques qui permettent d'isoler des opérations financières et des comptes sur la blockchain appartenant à un pseudonyme. Cela peut permettre à une personne d'estimer la balance du pseudonyme en question et donc au final de l'identifier. Nous pensons aux services qui proposent la création d'un portefeuille en ligne ou d'une plateforme de change, qui permet d'associer l'identité d'un utilisateur à son adresse publique voire aux mesures de lutte contre le blanchiment d'argent (le « *Know Your Customer* » du monde financier), qui ont précisément pour objet d'identifier les clients au moment d'une relation d'affaire.

Analyse d'impact

Il s'agit d'une analyse des impacts des traitements lors du recours à de nouvelles technologies, lorsque les traitements envisagés sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques. À ce moment, le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Dans la blockchain, les informations peuvent être remplacées par leur « *hash* ». Il s'agit d'analyser si le fait de déposer des « *hash* » sur une blockchain crée des risques pour les droits et libertés des personnes concernées. Il faudra par exemple que le responsable du traitement s'assure que les banques de données liées à ces *hash* soient sécurisées chez lui.

Consentement de l'utilisateur

Dans le cadre de l'utilisation de la blockchain, les consentements sont explicites car c'est l'utilisateur (ou quelqu'un mandaté à cet effet) qui réalise

l'empreinte du document. Il s'agira d'analyser, au cas par cas, si l'utilisateur a réalisé un acte positif clair permettant cet enregistrement sur la blockchain. Toutefois, cet enregistrement peut aussi rentrer dans la démarche des traitements licites car nécessaire à l'exécution d'un contrat accepté par la personne (et donc reposer sur un autre fondement légal).

Accès aux données et effacement

Dans la blockchain, les utilisateurs ont toujours accès au registre. Néanmoins, ils ne pourront jamais effacer une information déposée dans la blockchain. Il s'agit là d'une des caractéristiques principales de toute blockchain et de la difficulté première à concilier blockchain et RGPD.

Délégué à la protection des données

Le rôle du délégué à la protection des données sera de garantir la conformité des traitements de données avec les principes de protection de la sphère privée, tels que fixés par le RGPD, ainsi que de gérer les relations entre les personnes concernées (employés, clients) et les autorités de surveillance. Il faudra que l'un des administrateurs du registre de la blockchain assume cette fonction. Le poste de DPD sera plus évident à satisfaire dans le cas d'une blockchain fermée que dans le cas d'une blockchain ouverte ou publique.

Le privacy by design

Les blockchains publiques constituent une technologie *privacy by design* inédite pour protéger la vie privée des utilisateurs. En effet, elle impose le recours par défaut à la pseudonymisation et aux algorithmes de chiffrement. À ce titre, elle répond aux exigences du RGPD en termes de sécurité des données et permet de lutter contre les fuites massives de données qui font régulièrement la une des journaux.

Le transfert des données hors EU

Les blockchains ne sont pas détenues par un organisme ou autorité voire société. La particularité des blockchains est d'être décentralisée. Chaque intervenant d'une blockchain voit la même version de la blockchain. Dès lors, pour être sûr qu'il n'y a pas de transfert au sens du RGPD, il faut s'assurer que chaque personne qui voit/participe à la blockchain est située en Europe. Dès qu'un intervenant est situé hors Europe, il y a transfert au sens du RGPD.

Restriction du profilage

Le profilage des personnes et des données personnelles ne peut se réaliser qu'avec l'accord des utilisateurs. Seul l'utilisateur possède les mots de passe. Or, le montant des transactions ainsi que le temps passé à les réaliser peuvent révéler de considérables informations sur les utilisateurs de la blockchain concernée. On est très proche du profilage.

Décision automatisée

Le RGPD prévoit que la personne concernée « a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ».

Les exceptions à cette règle s'appliquent lorsque pareille décision automatisée est prévue par la loi (par exemple pour prévenir les fraudes) ou si c'est nécessaire pour conclure un contrat ou si la personne a donné son accord explicite. Toutefois, dans le cas des deux dernières hypothèses, il est prévu alors que la personne concernée peut « obtenir une intervention humaine de la part du responsable du traitement », exprimer son point de vue et contester la décision. Il s'agit ici du droit pour la personne concernée de recevoir une justification de la décision automatisée. Dès lors, même si un système est à 100 % automatisée/automatique est possible, il devra quand même toujours prévoir la possibilité pour la personne objet de cette décision de pouvoir faire appel à une personne humaine pour en recevoir la justification.

Dans le cas où la personne est liée par un « *smart contract* » automatique, elle a d'elle-même accepté de subir les conséquences de la future décision automatique, quelle qu'elle soit.

Cette acceptation peut-elle la priver, dans le cas où la décision automatique rendue est désavantageuse pour elle, du droit d'obtenir une intervention humaine ayant la capacité de renverser la décision automatique ?

Autrement dit, est-il possible dans un contrat (ici, un « *smart contract* » mais la problématique est la même s'il s'était agi d'un contrat habituel) de se priver de l'exercice d'un droit futur ?

La réponse à cette question dépendra de la qualification du droit octroyé aux personnes concernées à obtenir une intervention humaine ayant la possibilité de renverser une décision automatique.

Vu l'importance mise par l'Union européenne dans ce nouveau droit, nous pensons pouvoir considérer ce nouveau droit comme impératif.

Les dispositions impératives ont pour but de protéger une des parties, soit en lui octroyant d'office certains droits, soit en interdisant à l'autre partie de lui imposer certaines obligations.

La protection du consommateur par exemple procède de dispositions impératives.

Dès lors que ces règles impératives ont pour but de protéger une des parties au contrat, la partie protégée peut décider de renoncer à cette protection légale mais uniquement une fois la situation survenue.

Fiche de guidance n° 46
À tenir à l'œil !

Nous voudrions terminer par une Fiche de guidance prospective concernant les réglementations que vous devez tenir à l'œil dans les prochaines semaines voire mois en matière de protection des données à caractère personnel au sens large.

La matière est mouvante, tentaculaire et très difficile à saisir.

Tentons d'en circonscrire son futur. Gageons que ce que nous écrivons ici sera l'objet de Fiches de guidance prochaines.

A. Le RGPD

Le RGPD est un Règlement (ou plutôt une Réglective comme nous l'avons mentionnée dans une Fiche de guidance précédente), ce qui améliore la situation par rapport à la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Toutefois, il y a encore (et pour longtemps, voire toujours) 28 autorités de contrôle nationales chacune œuvrant dans un pays avec une culture et des sensibilités différentes. Il sera intéressant de voir comment le futur Comité européen de la protection des données (le CEPD) parviendra à créer une harmonisation ou une uniformisation en la matière et comment il parviendra à établir son autorité sur les 28 autorités de contrôle nationale. Son travail (qui il est vrai ne sortira pas de nulle part mais sera issu de l'excellent travail du Groupe de Travail « Article 29 ») sera primordial.

Il faut que les règles du RGPD soient interprétées de la même manière partout en Europe (voire dans le monde quand on voit l'influence des règles européennes en Afrique ou en Asie).

Comment les GAFA et autres sociétés américaines vont-elles appliquer les règles du RGPD est également une problématique à suivre. Il ne faut pas que les règles draconiennes du RGPD (en matière de *profiling* et de *big data* par

exemple) nuisent à l'économie européenne au bénéfice des Google et autres qui, alors qu'ils le doivent, ne les appliqueront pas. Y aura-t-il de la collaboration entre le CEPD et les services de la concurrence de la Commission européenne à ce sujet ? Dans combien de temps la Cour de justice rendra-t-elle son premier arrêt en rapport avec le RGPD (dans 10 ans quand on voit la lenteur de la justice) ?

Au sujet de la licéité des traitements fondés sur le prétendu consentement des citoyens européens, les autorités ne peuvent se contenter de miser sur la capacité des Européens d'autoriser ou non les pratiques de traitement parfois trop intrusives des entreprises.

Les documents résumant pour approbation les critères d'utilisation des données collectées sont souvent en effet d'une longueur et d'une complexité absurdes et la tâche devient impossible à gérer individuellement au fur et à mesure que les applications se multiplient.

La création du CEPD, instance régulatrice centralisée en la matière, capable de fixer des balises claires, de demander des comptes aux entreprises et de sévir au besoin est porteuse d'espoir et marque un pas dans la direction d'agir énergiquement pour mieux protéger la population.

Les données à protéger sont, il est vrai, personnelles, mais la réponse requise est sans aucun doute collective.

B. La proposition de Règlement *ePrivacy*

Nous ne développerons pas beaucoup ce point-ci puisque nous y avons consacré une Fiche de guidance particulière.

Pour plus de cohérence, la Commission européenne va-t-elle dans une dizaine d'années proposer un Règlement unique combinant les règles du RGPD et du Règlement *ePrivacy* ? Ce semblerait logique et empêcherait toute incohérence entre les deux corps de règles. La consécration (que nous espérons) du fait que le CEPD devra superviser tant le RGPD que le futur Règlement *ePrivacy* est une première étape allant dans ce sens.

C. Le futur Code des Communications Électroniques

Ce « Code » (qui n'en est pas vraiment un) est en réalité une Directive qui regroupe quatre anciennes Directives qui viendront à être remplacées par celle-ci. Beaucoup ont regretté que la Commission européenne n'ait pas proposé, dans son travail de réexamen, un Règlement plutôt qu'une Directive aux transpositions nationales on le sait fort diverses.

La nouvelle Directive consiste en une refonte horizontale des quatre directives en vigueur en matière de communications électroniques (la directive 2002/21/CE « cadre », la directive 2002/20/CE « autorisation », la directive 2002/19/CE « accès » et la directive 2002/22/CE « service universel » toutes datées du 7 mars 2002), qu'elle regroupe au sein d'une seule et unique directive.

Le Code régira les entreprises, les opérateurs de télécommunications traditionnels ainsi que dorénavant les prestataires dits de services par contournement (« *over the top* » – OTT), qui proposent une large panoplie d'applications et de services, y compris des services de communications, sur l'internet. Il s'agit des mêmes OTT qui seront aussi bientôt soumis aux règles en matière d'*ePrivacy*.

Notons que le travail législatif européen sur cette proposition de Directive va de pair avec celui en rapport avec un réexamen des règles régissant le BEREC (groupe des régulateurs européens en matière de communications électroniques où la Belgique est représentée par l'IBPT et le France par l'ARCEP). Il s'agit là d'une proposition de Règlement datée du 14 septembre 2016. À voir dès lors, la coopération qui va se mettre en place entre le BEREC et le CEPD.

D. La mise en œuvre de la Directive NIS

Là aussi, nous n'entrerons pas dans le détail du sujet et renvoyons le lecteur à la fiche de guidance que nous y avons consacrée.

E. La mise en œuvre progressive de la Directive PSD2

Sous le vocable « PSD2 » se cache la Directive révisée concernant les services de paiement. La directive PSD2 constitue un prolongement de la première Directive sur les services de paiement (PSD) de 2007 qui a installé le standard de transfert bancaire européen SEPA. L'objectif de PSD2 est toujours de réguler les activités des prestataires de services de paiement et de créer un cadre harmonisé à travers toute l'Europe.

La directive PSD2 précise (e.a.) que toute entreprise qui fournit et conserve des informations sur des comptes clients doit rendre ces dernières accessibles à des tiers, notamment à des prestataires de paiement mobile (les « *Payment Initiation Service Providers* » ou PISP) ou d'agrégation de comptes (les « *Account Information Service Providers* » ou AISP), sous réserve que le client leur en ait donné l'autorisation. Une telle mesure contraindra les banques à ouvrir à des tiers l'accès aux données de leurs comptes clients via des interfaces

de programmation applicative (API). PSD2 entend aussi règlementer les fournisseurs tiers (les « *Third Party Providers* » ou TPP) qui auront dès lors aussi accès aux données clients des banques. Les TPP seront soumis à leurs propres exigences en matière d'information, de transparence et de sécurité des paiements. Ils devront fournir leurs services dans une infrastructure totalement sécurisée.

Cette Directive contraindra fortement les actuels acteurs du secteur des paiements à repenser leur mode de fonctionnement.

Nous sommes curieux et impatients de voir si le « consentement explicite » requis par PSD2 pour qu'un prestataire de paiement (une banque ou un TPP par exemple) puisse traiter les données de ses clients pour des finalités autres que la fraude sera interprété différemment que le « consentement explicite » du RGPD.

Beaucoup se demande aussi si un TPP qui a obtenu l'accord d'un consommateur pour traiter ses données dans un but d'agrégation de ses comptes bancaires doit obtenir un second accord de la part du consommateur pour lui fournir d'autres services (comme des propositions d'investissements, des comparaisons de prix, etc.). Ce point est en lien direct avec la problématique des traitements compatibles ou incompatibles avec la finalité première pour lesquelles des données ont été collectées.

Comment les futurs TPP (essentiellement des nouvelles FinTechs) pourront-ils créer la confiance suffisante que pour obtenir le consentement des consommateurs et donc leurs données ?

On le voit, les problématiques sont les mêmes. Espérons que les Lignes directrices des différents régulateurs ainsi que les décisions de justice qui arriveront sûrement par après soient convergentes.

F. Le Brexit

Le monde des affaires est inquiet par rapport au Brexit et au sort du RGPD en 2019. Le gouvernement anglais a affirmé qu'il implémenterait avant mai 2018 les règles du RGPD dans sa législation. Ce travail devrait faciliter le vote d'une future décision d'adéquation entre l'Europe et la Grande-Bretagne (Ecosse y compris ?).

G. Les nouvelles technologies

Nous avons parlé de la blockchain et de la DLT, des cryptomonnaies, des objets connectés et de l'internet des objets (IoT) qui créent et traitent de plus en plus de données à caractère personnel mais aussi à caractère non personnel au bénéfice des grandes sociétés multinationales.

L'émergence et la banalisation de ces nouvelles technologies (pensons au développement des voitures connectées et intelligentes capables de recueillir et de transmettre (à qui ?) une foule de renseignements sur le comportement des conducteurs) ne doivent pas se faire au détriment de la protection de nos données personnelles et de nos libertés (d'expression, de mouvement, etc.).

Il faudra bien suivre et comprendre les futures Lignes directrices des différents régulateurs qui auront à s'en préoccuper (et ils sont nombreux !).

H. *Open data* et données à caractère non personnel

L'*open data* concerne la publication et la mise en ligne des données produites et détenues par les administrations publiques. Et elles sont pléthoriques mêmes s'il ne s'agit pas à chaque fois de données à caractère personnel. En effet, comme le rappelle la CNIL sur son site, « la majorité des informations du secteur public mises à disposition des internautes ne comportent aucune donnée personnelle. Il peut s'agir, par exemple, de données liées au fonctionnement budgétaire et quotidien d'un service public, de statistiques, de cartographies et de localisation, de données liées à l'organisation d'évènements culturels et sportifs, d'informations touristiques, de mesures sur la qualité environnementale, etc. ».

La mise en ligne dans une forme la plus réutilisable possible de ces données permet le développement de nouvelles solutions technologiques ou l'amélioration de pratiques existantes.

Toutefois, il convient aussi de respecter l'anonymat des personnes mentionnées dans les documents et informations publiques (décisions de jurisprudence ou les données de santé par exemple). La mise en ligne de la plateforme data.gouv.fr, où plus de 20 000 jeux de données sont aujourd'hui disponibles, fait de la France un des États les plus en pointe du mouvement d'ouverture des données publiques.

Espérons que l'ensemble des États européens suivront le même mouvement : une mise en ligne automatique des données publiques tout en veillant à une anonymisation des personnes mentionnées dans les documents et une impossibilité de réidentification. Et ce même si on sait qu'une anonymisation certaine est très difficile car avec les milliards d'informations aujourd'hui disponibles, certains algorithmes poussés peuvent réidentifier des personnes données.

Annexe 1
Bonus 1 : Pourquoi faut-il que les sociétés soient au plus vite conformes au RGPD ?

La non-conformité de toute société pourrait avoir deux conséquences :

1. les amendes possibles et élevées ;
2. un risque réputationnel quand le temps viendra de comparer les sociétés entre elles (des associations se sont spécialisées dans ces analyses intra voire aussi cross-sectorielles). Une seule violation pourrait modifier considérablement la perception du public quant à la société mise ainsi en évidence.

Les sociétés vont devoir se rendre compte que non seulement les données qu'elles détiennent ou vont prochainement acquérir servent à augmenter ses activités mais aussi que ces données sont potentiellement des risques si ces données sont mal protégées.

Les sociétés vont devoir dès lors « profiter » du RGPD et de leur travail de mise en conformité pour élever leur sécurité informatique.

Le travail de mise en conformité en ce qu'il va obliger les sociétés à revoir leur infrastructure informatique, à la modifier et à la moderniser va leur permettre d'augmenter leur productivité, de réduire leurs coûts et surtout de remplir pleinement le contrat de confiance qu'elles ont envers leurs clients et les données que ces derniers ne font que leur prêter.

La sécurité informatique et la confiance des consommateurs vont aller de plus en plus ensemble. Cette sécurité va devenir un réel argument marketing pour différencier les sociétés entre elles. Il s'agirait aussi de ne pas prétendre que l'on protège correctement les données alors que tel n'est pas le cas. Une erreur ou un mensonge sera rapidement décelé par les concurrents, par les autorités de contrôle ou par le marché.

Plus qu'un ensemble de contraintes, les entreprises peuvent voir ce changement imposé comme un générateur de confiance, donc de croissance.

Protéger la confidentialité et la sécurité des données personnelles va devenir (voire est déjà) un élément décisif de la relation client. À l'heure de l'interconnexion généralisée des systèmes informatiques, de l'ouverture des

réseaux, du cloud, des objets connectés, qui oserait confier ses informations personnelles, bancaires, médicales, familiales, etc. à un acteur dont la fiabilité numérique n'est pas garantie ?

Sans cybersécurité, pas de confiance. Et sans confiance, impossible d'adopter de nouvelles technologies, de poursuivre la transformation numérique de nos sociétés et de bénéficier des opportunités qu'elle génère, notamment en matière de Big Data. La confiance reconnue conditionne la croissance générée par la révolution numérique.

La cybersécurité n'est pas une fin en soi : gardons plutôt à l'esprit qu'elle va permettre aux sociétés d'entreprendre ! Le RGPD n'est pas uniquement un compte à rebours nécessitant la coopération de nombreuses entités au sein des organisations (services informatiques, juridiques, financiers) et le respect d'obligations nouvelles (par exemple, le recrutement d'un délégué à la protection des données). Si sa mise en œuvre peut sembler un travail conséquent, il ne devrait être qu'un jalon d'une stratégie numérique devant intégrer pleinement la cybersécurité dès la conception des systèmes et tout au long de leur cycle de vie.

Annexe 2

Bonus 2 : Aperçu de mesures à entreprendre pour être conforme au RGPD

1. Agir maintenant ! Ne surtout pas attendre que le RGPD entre en vigueur !

   OK : ❑

   NOK : ❑

2. Réaliser une cartographie complète des données qui sont possédées et traitées par la société en question (= une cartographie des données et des traitements réalisés en allant interroger les services et les personnes adéquates de la société) (un « *mapping* »).

   OK : ❑

   NOK : ❑

3. Analyser dorénavant et avant chaque traitement, la base juridique du traitement que l'on a en tête.

   Attention, si la base juridique est le consentement/consentement explicite, le RGPD contient de nouvelles exigences (article 7 du RGPD). Si la base juridique sont les intérêts légitimes de la société, une analyse pondérée est à réaliser, la personne concernée doit en être informée et doit être informée qu'elle peut s'y opposer (la société doit faire en sorte de pouvoir effectivement obéir aux indications de la personne qui s'oppose). Si le traitement concerne des données dites « particulières » (des données médicales par exemple), le consentement devra être explicite.

   OK : ❑

   NOK : ❑

4. Auparavant, les sociétés devaient juste gérer le dernier choix de leurs clients en matière de consentement ainsi que gérer les procédures de désinscription (souvent des désinscriptions en ligne concernant le marketing direct). Dorénavant, les sociétés devront aussi pouvoir démontrer que le consentement a été donné. Elles devront archiver une trace de ce consentement. Si une société utilise plusieurs types de collecte de consentement (électroniques, par l'intermédiaire d'un rendez-vous physique ou via une conversation téléphonique), il serait bon que les sociétés gardent une trace des différentes formulations de consentement.

   OK : ❑

   NOK : ❑

5. Informer au moment opportun, correctement et de manière transparente les personnes concernées de leurs droits.

   Ce moment va dépendre du fait que les données ont été collectées directement de la personne concernée ou bien via un tiers. Cette information se réalisera en ce qui concerne les données collectées directement auprès de la personne concernée via un « *Privacy Statement* ». Ce « *Privacy Statement* » qui doit normalement déjà exister devra être mis en conformité avec le RGPD.

   OK : ❑

   NOK : ❑

6. Avoir les bons outils informatiques pour permettre aux personnes concernées de pouvoir exercer les droits qu'elles ont du RGPD. Ces droits vont dépendre de la base juridique du traitement et ils ne sont pas absolus.

   Attention aux nouveaux droits comme le droit à l'oubli et le droit à la portabilité des données et au fait qu'il faudra répercuter l'exercice des droits auprès des sous-traitants.

   OK : ❑

   NOK : ❑

7. Dans le cas où la société traite des données relatives à des enfants, la société ne doit pas oublier que le consentement de l'enfant n'est licite que s'il a plus de 16 ans.

   Lorsque l'enfant est âgé de moins de 16 ans, le traitement ne sera licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.

Les sociétés devront implémenter des outils informatiques afin d'être sûres que l'enfant a bien 16 ans et plus pour être certaines que le consentement a été valablement donné et de bien recueillir le consentement des parents dans le cas où l'enfant n'a pas 16 ans. La société pourrait, par exemple, demander à l'enfant l'adresse électronique de ses parents pour envoyer un mail de consentement auxdits parents.

Les États membres peuvent prévoir que l'enfant peut donner un consentement licite pour les âges compris entre 13 et 16 ans. Pour les enfants en-dessous de 13 ans, l'accord des parents sera donc toujours requis.

OK : ❑

NOK : ❑

8. Si la société prend des décisions automatisées (en ce compris du profilage), elle doit bien se rendre compte que, dorénavant, il y aura deux types de profilage :
   a) le profilage réalisé à des fins de prospection (marketing direct). Dès lors :
      i. la société devra informer la personne concernée que la société réalise bien du profilage à des fins de prospection (information donnée généralement via la *Privacy Statement*) ;
      ii. la société devra informer, aussi via sa *Privacy Statement*, que la personne concernée peut s'opposer à ce profilage ;
      iii. dans le cas où une personne refuse de recevoir du direct marketing de la société, elle ne pourra plus faire l'objet de profilage à des fins de prospection.
   b) le profilage produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire (exemple : un *scoring* automatique concernant l'obtention automatique d'un crédit en ligne) :
      i. à moins que le profilage soit nécessaire pour conclure un contrat ou requis par une disposition légale, la société devra obtenir le consentement explicite de la personne concernée. Ce consentement explicite devra être archivé ;
      ii. lorsque le profilage est nécessaire pour conclure un contrat ou fondée sur le consentement explicite de la personne concernée, le responsable du traitement devra mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, en ce compris le droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

OK : ❑

NOK : ❑

9. Analyser les contrats que possède la société avec ses sous-traitants afin de rendre conforme ces contrats avec les nouvelles exigences de l'article 28 du RGPD. Prévoir la manière dont va se dérouler la coordination avec les sous-traitants en matière de violation de données personnelles (« *data breach* ») et de portabilité des données.

   OK : ❑

   NOK : ❑

10. Si la société réalise des transferts hors UE, bien voir si le transfert hors UE peut se réaliser au sens du RGPD (il s'agit ici de réviser les « *data flow* » de la société).

    OK : ❑

    NOK : ❑

11. Nommer un DPD si c'est obligatoire et voire s'il ne faut pas quand même en nommer un dans le cas où ce n'est pas obligatoire.

    OK : ❑

    NOK : ❑

12. Chercher à bien appréhender et cerner les données traitées par la société dans le but d'en maîtriser la gestion de bout en bout : de quel type de données s'agit-il ? s'agit-il de données particulières ? Où sont-elles hébergées ? Où transitent-elles et par quel(s) moyen(s) ? Comment sont-elles protégées ?

    Il s'agit ici de réaliser un audit complet des données qui tiendra aussi compte des services de cloud (et de leur localisation) utilisés par la société (qu'ils aient été approuvés ou non par la direction – ce que l'on appelle le « *shadow IT* »).

    OK : ❑

    NOK : ❑

13. Implémenter les bonnes mesures de protection (sécurité) surtout en ce qui concerne les données sensibles possédées et traitées par la société.

    Ne pas oublier que les données pseudonymisées sont encore des données personnelles.

Ce sont les données réellement rendues anonymes (sans possibilité aucune de réidentification) qui sortent du champ d'application du RGPD. Ne pas oublier de se poser des questions par rapport aux services de cloud utilisés par la société : quel est le niveau de chiffrement des données stockées appliqué par le service de cloud ? qui en possède « les clés » ? quelles sont les certifications de *datacenter* présentes ? le service partage-t-il les données personnelles avec des tierces parties ?

OK : ❑

NOK : ❑

14. Implémenter en interne le registre des activités de traitement des données à caractère personnel de l'article 30 du RGPD.

OK : ❑

NOK : ❑

15. Implémenter aussi un registre des violations des données où seront enregistrés même les violations non notifiées à l'autorité de contrôle de données personnelles.

Ce registre contiendra une description de la violation, sur quoi portait-elle, qui a été impacté, les mesures prises pour y pallier dans le futur et les conséquences de ces mesures.

OK : ❑

NOK : ❑

16. Implémenter un registre des mesures de sécurité prises afin de pouvoir démontrer l'adéquate sécurité et protection de nos données en fonction des risques de chaque traitement (« *risk-based approach* »).

OK : ❑

NOK : ❑

17. Implémenter un registre des analyses pondérées réalisées pour chaque traitement dont la base juridique est les intérêts légitimes de la société.

OK : ❑

NOK : ❑

18. Implémenter un registre de l'exercice des droits des personnes concernées.

En effet, l'exercice des droits est gratuit pour les personnes concernées. Le responsable du traitement peut exiger le paiement de frais

raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées ; ou refuser de donner suite à ces demandes lorsqu'il considère que les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif. La création de ce registre des droits l'aidera à pouvoir démontrer le caractère manifestement infondé ou excessif de la demande.

OK : ❑

NOK : ❑

19. Concevoir un processus qui devrait rapidement permettre à la société de réaliser une analyse d'impact relative à la protection des données (une AIPD). Préalablement au traitement et si la société estime que le traitement risque d'engendrer des (hauts) risques pour les personnes concernées, elle devra réaliser une AIPD (qui peut déboucher sur la consultation de l'autorité de contrôle de données personnelles nationale).

OK : ❑

NOK : ❑

20. Implémenter un système de gestion des potentielles violations en matière de données à caractère personnel.

OK : ❑

NOK : ❑

21. Avoir un système d'archive et de documentation afin de pouvoir répondre rapidement et adéquatement aux questions des personnes concernées et de l'autorité de contrôle de protection des données personnelles compétente.

Il faudra pouvoir tout documenter sous l'empire du RGPD (par exemple) :

- bien archiver les consentements,
- en matière d'AIPD : pourquoi la société n'a pas fait une AIPD et si la société en a fait un tout son déroulement,
- en matière de violation de données à caractère personnel : si la société n'a pas prévenu l'autorité de contrôle de données personnelles, pourquoi ?
- si la société a choisi les intérêts légitimes comme base juridique, l'analyse pondérée par rapport aux droits de la personne concernée,

– etc.

OK : ❑

NOK : ❑

22. Ne conserver les données sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (écriture d'une bonne « *Retention Policy* »).

OK : ❑

NOK : ❑

23. Former les employés et écrire les différentes guidances internes en la matière.

Citons :

– la guidance interne en cas de violation de données personnelles (« *data breach* ») (que faire ? Qui contacter ?) ;
– les guidances internes pour bien répondre à une requête d'une personne concernée, d'une autorité de contrôle des données personnelles ;
– comment implémenter la *privacy by design* et *by default* dans l'ensemble des projets de la société ;
– la guidance en matière de rétention de données ;
– comment prévenir des parties tierces dans le cas où la personne concernée a demandé l'effacement de ses données, etc.

Un bon accompagnement des employés est fondamental.

OK : ❑

NOK : ❑

24. Si la société fait partie d'un groupe de sociétés, il s'agit de réfléchir à introduire des règles d'entreprise contraignantes (« BCR »), à adhérer à un code de conduite, à se faire certifier et à mutualiser le DPD.

OK : ❑

NOK : ❑

25. Les sociétés devraient rapidement déterminer quelle est leur « *lead supervisory authority* » qui va les contrôler.

Cette détermination peut être réalisée par la localisation du principal établissement de la société. Toutefois, cet examen peut parfois être difficile dans le cas où les décisions de différents traitements sont prises

dans plusieurs États membres. Dans le cas où la société hésite quant à la détermination de sa « *lead supervisory authority* », elle devrait au plus vite cartographier ses traitements pour pouvoir déterminer avec exactitude où sont réellement prises les décisions à propos de chaque traitement. La société devrait aussi déterminer quelles sont les autres autorités de contrôles concernées par ses activités.

OK : ❑

NOK : ❑

Annexe 3
Glossaire des termes et expressions les plus utilisés dans la matière de la protection des données à caractère personnel

Autorité de contrôle : Autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51 du RGPD.

Biométrie : Ensemble de techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques ou comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne.

Contrôleur européen de la protection des données (CEPD) : Autorité de contrôle indépendante ayant pour mission d'assurer que les institutions et organes européens respectent le droit à la vie privée et à la protection des données personnelles lorsqu'ils traitent des données et élaborent de nouvelles politiques.

Cloud computing : En français, l' « informatique dans les nuages ». L'expression fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé et localisable mais dans un nuage (cloud) composé de nombreux serveurs distants interconnectés.

Cookies : Les cookies sont des traceurs déposés et lus lors de la consultation d'un site Internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel. Les cookies et autres traceurs ont généralement pour finalité d'analyser la navigation et la fréquentation du site Internet en question.

Data scientists (ex-dataminers): On appelle « *data scientists* » les professionnels ou les agences qui développent ou utilisent de nouveaux outils informatiques

(généralement en mode open source) permettant d'exploiter intelligemment, et de plus en plus en temps réel, d'énormes flux extrêmement variés de données et d'informations afin de faire du prédictif.

Délégué à la protection des données (« *Data Protection Officer* » – DPD): Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39 du RGPD.

Destinataire : La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

Donnée à caractère personnel (une) : Il s'agit de toute information se rapportant à une personne physique (pas morale). L'information doit se rapporter à une personne physique identifiée (on sait qui c'est) voire à une personne physique qui est identifiable. Une personne physique sera considérée comme étant identifiable à partir du moment où elle peut être identifiée, que l'identification soit directe ou indirecte. Cette identification (directe ou indirecte) peut se réaliser, notamment, par référence à un identifiant comme un nom, un numéro d'identification (dans une liste), des données de localisation ou un identifiant en ligne. L'identification peut également s'effectuer par renvoi à un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de la personne physique. La définition est donc extrêmement large.

Finalité du traitement : Objectif principal d'un traitement de données à caractère personnel. Exemples de finalité : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, gestion des sinistres (courtiers), etc.

Groupe de Travail « Article 29 » : Groupe de Travail prévu à l'article 29 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Le Groupe de Travail rassemble les représentants des autorités indépendantes de protection des données nationales des États de l'Union européenne. Sa mission est de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays tiers

et de conseiller la Commission européenne sur tout projet ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles. Il sera remplacé en mai 2018 par le Comité européen de la protection des données (CEPD) (attention, il s'agit, en français, des mêmes abréviations que celles relatives au Contrôleur européen de la protection des données de Butarelli)

Limitation du traitement : Marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur.

Open Data : Expression désignant un mouvement né en Grande-Bretagne et aux États-Unis, d'ouverture et de libre accès des données produites ou collectées par les services publics aux fins de leur réutilisation. Les données ouvertes (ou Open Data) sont des informations accessibles librement et gratuitement, sous la forme de fichiers respectant des formats interopérables.

Pays adéquats : Les données à caractère personnel peuvent être transférées des 28 États membres de l'UE et de trois États membres de l'EEE (Norvège, Liechtenstein et Islande), vers le pays tiers concerné sans qu'il soit nécessaire de prévoir d'autres garanties. La Commission européenne a constaté à ce jour qu'Andorre, l'Argentine, le Canada (organisations commerciales), les Îles Féroé, Guernesey, Israël, l'Île de Man, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay prévoient une protection adéquate. La situation des États-Unis est réglée via le *Privacy Shield*. Le *Privacy Shield* est un mécanisme d'auto-certification pour les entreprises établies aux États-Unis qui a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données à caractère personnel transférées par une entité européenne vers des entreprises établies aux États-Unis. Ce mécanisme est par conséquent considéré comme offrant des garanties juridiques pour de tels transferts de données.

Personne concernée : Il s'agit de la « personne physique identifiée ou identifiable » comme vu précédemment pour « Donnée à caractère personnel ».

Portabilité : Le droit à la portabilité des données permet aux personnes concernées d'exiger des responsables de traitement la transmission de leurs données à caractère personnel à un autre responsable de traitement, sans que le responsable de traitement ayant initialement collecté les données puisse s'y opposer.

Privacy Shield : Mécanisme par lequel une société de droit américain est réputée appliquer un minimum standard de principes de protection de la vie privée par son adhésion, renouvelée annuellement, à une liste dédiée auprès du Ministère du commerce des États-Unis. Seul cet agrément autorise l'entreprise de droit américain à traiter les données à caractère personnel collectées au sein de l'UE.

Pseudonymisation : Il s'agit de traiter les données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

Règles d'entreprise contraignantes (« *Corporate Binding Rules* » – BCR) : Règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe.

Registre des activités de traitement : Le registre des activités de traitement répertorie les informations relatives aux caractéristiques des traitements mis en œuvre par le responsable de traitements.

Responsable du traitement : Par responsable du traitement, le RGPD vise la personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

Responsables conjoints du traitement : Hypothèse dans laquelle plusieurs responsables déterminent conjointement les finalités et les moyens du traitement.
Il n'est pas nécessaire que les responsables de traitements participent de façon égale à la détermination des finalités et moyens du traitement pour être considérés comme responsables conjoints du traitement : la participation des parties à la détermination conjointe d'un traitement peut revêtir différentes formes et n'est pas nécessairement partagée de façon égale. En effet, lorsqu'il y a pluralité d'acteurs, ils peuvent entretenir une relation très proche (en partageant, par exemple, l'ensemble des finalités et des moyens d'une opération de traitement) ou, au contraire, plus distante (en ne partageant que les finalités ou les moyens, ou une partie de ceux-ci). En effet, pour qu'une personne puisse être considérée comme un responsable du traitement, il n'est pas nécessaire que cette personne dispose d'un pouvoir de contrôle complet sur tous les aspects du traitement. Pour être un responsable du traitement, il ne faut pas disposer d'un pouvoir de contrôle complet sur tous les aspects du traitement. Dès lors, l'éventail de typologies de responsables conjoints est particulièrement large et leurs conséquences juridiques doivent être évaluées, avec une certaine souplesse pour tenir

compte de la complexité croissante de la réalité des traitements de données actuels. Attention : le simple fait que différents acteurs coopèrent dans le traitement de données à caractère personne ne signifie pas nécessairement qu'ils sont responsables conjoints. En effet, un échange de données entre deux parties, sans partage des finalités ou des moyens dans un ensemble commun d'opérations, doit être considéré uniquement comme un transfert de données entre des responsables distincts.

Sous-traitant : Personne physique ou morale, d'une autorité publique, d'un service ou d'un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Traitement de données : Opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Transferts de données hors Union européenne : On parle de transfert de données à caractère personnel lorsque des données sont transférées depuis le territoire européen vers un ou des pays qui n'appliquent pas les dispositions du RGPD (il s'agit des pays ni membres de l'Union européenne, ni membres de l'Espace économique européen). Le transfert peut s'effectuer par communication, copie ou déplacement de données, par l'intermédiaire d'un réseau (ex : accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de support (ex. d'un disque dur d'ordinateur à un serveur).

Violation de données à caractère personnel : Violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Annexe 4
Bibliographie (très) sélective

A. Ouvrages

Rapport Big data – Les Big Data examinées sous l'angle du Règlement général sur la protection des données : quelques recommandations pour une bonne utilisation, une publication de la Commission (belge) sur la protection de la vie privée (CPVP), Éditions Politeia SA, Bruxelles, 2017

Gérard HAAS, *Le RGPD expliqué à mon boss*, Éditions Kawa, France, 2017

Rubin Sfadj et Élodie Granger, *Réussir votre mise en conformité GDPR – Guide pratique*, Paris, Proposition 47 Production SAS, 2017

Protection des données personnelles – Se mettre en conformité d'ici le 25 mai 2018, Montrouge, France, Éditions législatives, 2017

Les données génétiques, Point CNIL, Paris, La documentation française, 2017

Le Data Protection Officer – Une fonction nouvelle dans l'entreprise, Bruylant, Collection Minilex, 2017

Vers un droit européen de la protection des données ?, Bruxelles, Larcier, 2017

Yung Shin Van der Sype, *Naar een geïntegreerde privacybescherming in de onderneming*, Mechelen, Wolters Kluwer, 2017

Laurent Leloup, *Blockchain – La révolution de la confiance*, Paris, Eyrolles, 2017

Stéphane Loignon, *Big Bang et Blockchain,* Paris, Tallandier, 2017

Règlement européen sur la protection des données – Textes, commentaires et orientations pratiques, Bruxelles, Larcier, 2016

Enjeux européens et mondiaux de la protection des données personnelles, Bruxelles, Larcier, 2015

Benjamin Docquir, *Le droit de la vie privée*, Bruxelles, Larcier, 2008

B. Revues

« Data Protection – L'impact du GDPR en assurance », *Dossier du Bull. Ass.*, Kluwer, 2017

Valérie Verbruggen, « Mise en œuvre du Règlement général sur la protection des données personnelles : coup de projecteur sur certaines nouvelles obligations à charge des responsables de traitement et des sous-traitants », *Orientations*, 2017/5, p. 2 et s.

Carolyne Vande Vorst, « Algemene verordening gegevensbescherming : vijf nieuwigheden van dichterbij bekeken », *Cah. Jur.*, 2016/4, p. 75 et s.

Tim Van Canneyt & Gaëtan Goossens, « The General Data Protection Regulation : 10 things company lawyers should know », *Cah. Jur.*, 2016/1, p. 1 et s.

Cécile De Terwangne, Karen Rosier & Bénédicte Losdyck, « Ligne de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.* n° 62/2016, p. 5

C. Lignes directrices (« Guidelines ») officielles

Voyez le site de la Commission de la Protection de la Vie Privée : www.privacycommission.be

Voyez le site de la CNIL : www.cnil.fr

Voyez le site du Groupe de Travail « Article 29 » : http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Voyez le site du Contrôleur européen de la protection des données (CEPD) : https://edps.europa.eu/edps-homepage_fr

Voyez le site de l'Agence nationale de la sécurité des systèmes d'information pour avoir plus d'informations en matière de sécurité : https://www.ssi.gouv.fr/