État : mars 2018

Le RGPD et ses conséquences sur la Suisse[1]

Sommaire

[1] *Avertissement : le présent texte fera l'objet d'ajouts et de modifications à la lumière de l'évolution de la réflexion aux niveaux national et européen. En effet, des clarifications sont en cours afin de connaître la position et l'interprétation des autorités de référence et de contrôles (G29, Commission européenne, autorités de contrôle des États membres de l'Union).*

Introduction

En janvier 2012, la Commission européenne a proposé un ensemble de mesures législatives afin d'actualiser et moderniser les règles contenues dans la directive de 1995 sur la protection des données (Directive 95/46/CE) et dans la décision-cadre de 2008 relative à la protection des données traitées dans le cadre de la coopération policière et judiciaire en matière pénale (Décision-cadre 2008/977/JAI). Cette réforme vise à créer un ensemble de règles uniformes à travers l'UE adaptées à l'ère numérique, à améliorer la sécurité juridique et à renforcer la confiance des citoyens et entreprises dans le marché unique du numérique. La réforme comprend une Communication exposant les objectifs de la Commission, ainsi que deux propositions législatives: un Règlement général sur la protection des données et une Directive spécifique pour le domaine de la police et de la justice.

En date du 14 avril 2016, le Parlement européen a finalisé plus de quatre ans de travaux en approuvant les textes proposés. Les règles issues du Règlement général sur la protection des données seront directement applicables dans tous les États membres à partir du 25 mai 2018. Les pays de l'UE auront jusqu'au 6 mai 2018 pour transposer les dispositions de la Directive dans leur législation nationale.

Le règlement général sur la protection des données (RGPD)

Le Règlement (UE) 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, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données ou RGPD) a été approuvé le 14 avril 2016 par le Parlement européen et entrera en vigueur **le 25 mai 2018**. À partir de cette date, le RGPD sera directement applicable à tous les acteurs actifs sur le territoire de l'Union européenne. En effet, dans le droit de l'Union européenne, un règlement est obligatoire dans tous ses éléments dès son entrée en vigueur (il ne pourra pas s'appliquer de manière sélective). Il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres, contrairement à la directive. Les nouvelles règles consistent à donner aux citoyens plus de contrôle sur leurs données personnelles, à responsabiliser davantage les entreprises tout en réduisant leurs charges déclaratives et à renforcer le rôle des autorités de protection des données. Ce texte de référence en Europe aura des répercussions directes sur un grand nombre d'entreprises suisses.

Champ d'application matériel (art. 2 RGPD)

Par rapport à la Directive 95/46/CE, le champ d'application matériel n'a pas changé sur le principe. Le RGPD s'applique à tout *«traitement de données personnelles, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel qui sont contenues ou pourraient être contenues dans un fichier»* (art. 2 § 1 RGPD). Il concerne toutes les données personnelles se rapportant à des personnes physiques identifiées ou identifiables et ne fait pas de distinction qu'il s'agisse d'un traitement mis en œuvre par une personne physique ou une personne morale de droit

public ou privé. L'article 2 § 2 RGPD prévoit quatre exceptions ; le RGPD « ne s'applique pas *« au traitement effectué :*

a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ;
b) 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 ;
c) par une personne physique dans le cadre d'une activité strictement personnelle ou domestique ;
d) 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. »

Le RGPD couvre le traitement des données personnelles concernant les personnes physiques quelle que soit la nationalité ou la résidence de ces personnes. Cela signifie que lorsque les données personnelles d'une personne physique domiciliée en Suisse sont traitées dans un pays membre de l'Union européenne, ces dernières bénéficieront de la couverture du champ d'application du RGPD.

Champ d'application territorial (art. 3 RGPD)

Par rapport à la Directive 95/46/CE, le champ d'application a été étendu et contient désormais le **critère du ciblage du public du traitement des données (application extraterritoriale)**. Par ailleurs, cette extension est conforme à la jurisprudence de la Cour de justice de l'Union européenne (CJUE), qui en 2014 s'était prononcée en faveur de l'application extraterritoriale de la Directive dans l'affaire Google Spain (C-131-12).

L'article 3 RGPD dispose ce qui suit :

1. *Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.*
2. *Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:*
   a) *à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ;* ***ou***
   b) *au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.*
3. *Le présent règlement s'applique 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.*

L'application du RGPD dépend donc des deux critères de rattachement suivants :

1. **Le critère de l'établissement** (= lieu d'établissement du responsable du traitement ou d'un sous-traitant ; art.3 § 1) : le responsable de traitement ou le sous-traitant est établi **dans l'Union européenne**. Dans ce cas, le règlement s'applique d'office que le traitement ait lieu ou non dans l'Union. Dans l'affaire Weltimmo c. NAIH (C-230/14), la CJUE a interprété la notion d'établissement de manière relativement large et flexible.

2. **Le critère du ciblage** (= le lieu de situation des personnes concernées par le traitement ; art. 3 § 2) : le responsable du traitement est établi **en dehors** de l'Union européenne mais ses activités de traitement concernent l'offre de biens ou services à des personnes concernées qui se trouvent sur le territoire de l'Union soit les activités de traitement concernent la surveillance des comportements de ces personnes concernées pour autant que ce comportement a lieu au sein de l'Union européenne. Dans ce dernier cas de suivi du comportement, le législateur européen fait principalement référence au suivi des internautes. **En pratique, le RGPD devrait s'appliquer lorsqu'un résident européen, peu importe sa nationalité, sera directement visé par un traitement de données.**

Dans le cadre de l'appréciation de la soumission au Règlement, il faudra toujours tenir compte du cas d'espèce et notamment de l'intention du responsable de traitement d'offrir des biens ou services à des personnes se trouvant sur le territoire de l'Union ou encore de surveiller le comportement de ces derniers.

Droits des personnes concernées

L'un des buts de la réforme européenne est d'octroyer **d'avantage de contrôle et de visibilité** aux personnes concernées. L'article 12 RGPD oblige le responsable de traitement à prévoir des procédures et des mécanismes permettant à la personne concernée d'exercer ses droits. Il consacre le principe de transparence : toute information adressée au public ou à la personne concernée doit être aisément accessible et facile à comprendre dans une forme concise et transparente, et formulée en termes simples et clairs – spécialement à l'égard d'un enfant. En règle, les informations seront fournies par écrit et sans frais. Le Règlement prévoit également des délais de réactions maximum. Toutes les modalités énoncées par l'article 12 RGPD sont applicables à tous les droits prévus par le Règlement, à savoir :

- **Le droit à l'information** (articles 13 et 14 RGPD) Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes une série d'informations. Le responsable de traitement doit également lui fournir des informations lorsqu'elles n'ont pas été collectées auprès de la personne concernée.

- **Le droit d'accès** (article 15 RGPD)
  La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que ses données personnelles sont ou ne sont pas traitées et, lorsqu'elles le sont, elle a le droit d'obtenir l'accès auxdites données ainsi qu'à un certain nombre d'informations complémentaire prévues aux lettres a) à h). Ce droit comprend également celui d'obtenir une copie des données qui font l'objet d'un traitement.

- **Le droit de rectification** (article 16 RGPD)
  La personne concernée a le droit de demander que ses données soient rectifiées ou complétées, et ce dans les meilleurs délais.

- **Le droit d'effacement ou « droit à l'oubli »** (article 17 RGPD)
  La personne concernée a le droit de demander l'effacement de ses données, dans les meilleurs délais, si l'un des motifs du § 1 s'applique. Si les données de la personne concernée ont été transmises à d'autres entités, le mécanisme du « droit à l'oubli » s'enclenche : le responsable de traitement devra prendre toutes les mesures raisonnables pour informer les autres entités que la personne concernée a demandé l'effacement de tout lien vers ses données personnelles, ou de toute copie ou reproduction de celles-ci.

- **Le droit à la limitation du traitement** (article 18 RGPD)
  La personne concernée a le droit, dans certains cas prévus par la loi, d'obtenir du responsable du traitement la limitation de ses données. Lorsqu'une telle limitation est demandée, le responsable de traitement ne pourra plus que stocker les données. Aucune autre opération ne pourra, en principe, avoir lieu sur ces données personnelles.

- **L'obligation de notification du responsable** (article 19 RGPD)
  Cet article met en place une obligation de notification à charge du responsable de traitement qui l'oblige à communiquer à chaque destinataire des données toute rectification, effacement ou limitation du traitement

- **Le droit à la portabilité des données** (article 20 RGPD)
  La personne concernée a le droit de récupérer les données qu'elle a fournies au responsable de traitement, dans un format structuré, couramment utilisé et lisible par machine, et a le droit de transmettre ces données à un autre responsable du traitement, par exemple pour pouvoir changer de fournisseur de service. Ce droit ne peut être utilisé que si le traitement des données est basé sur le consentement de la personne concernée ou sur un contrat.

- **Le droit d'opposition** (article 21 RGPD)
  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'intérêt public ou l'intérêt légitime du responsable de traitement, y compris le profilage basé sur ces dispositions. La personne concernée a également le droit de s'opposer à ce que ses données soient traitées à des fins de marketing direct.

- **Le droit de ne pas être soumis à une décision individuelle automatisée** (article 22 RGPD)
  La personne concernée a le droit de ne pas être soumise à une décision résultant exclusivement d'un traitement automatisé produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. Le **profilage** y est expressément inclus.

- **Le droit à la communication d'une violation de données à caractère personnel** (article 34 RGPD).
  Le responsable de traitement est obligé de notifier à la personne concernée les violations de données susceptibles de l'exposer à un risque élevé à ses droits et libertés.

Le Règlement a en outre prévu une protection spécifique pour les enfants, ces derniers étant moins conscients des risques, des conséquences et de leurs droits en matière de protection des données. L'article 8 RGPD prévoit que lorsque des services de la société de l'information sont directement proposés à un enfant, le consentement au traitement des données de l'enfant doit être donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de cet enfant (les États membres peuvent librement fixer l'âge limite entre 13 et 16 ans).

Applicabilité aux entreprises suisses (art. 3 et 27 RGPD)

Il ressort du texte du Règlement et de ses considérants que le RGPD sera applicable aux entreprises suisses dans les cas prévus par le critère :

De l'établissement (article 3 § 1 ; considérant 22) :

- Traitement des données personnelles qui a lieu dans le cadre des activités **d'une succursale ou filiale[2] européenne d'une entreprise suisse** sur le territoire de l'Union ;

- **Sous-traitance[3] :** Traitement des données personnelles effectué par une entreprise suisse[4] en tant que sous-traitant pour le compte d'une entreprise européenne.

  Un sous-traitant sur le territoire de l'Union (ex. prestataire de services informatiques) qui traite des données personnelles pour une entreprise suisse sera soumis au Règlement peu importe qu'il traite des données de personnes concernées en Suisse ou dans l'Union (art. 3 § 1 RGPD). Il sera tenu de respecter les obligations spécifiques aux sous-traitants prévues par le Règlement (cf. articles 28, 30 § 2 et 37 RGPD) et les exigences découlant du droit suisse (cf. art. 10a LPD). Sa responsabilité est susceptible d'être engagée en cas de manquement. Cela ne signifie toutefois pas que le responsable de traitement en Suisse sera de ce fait soumis au Règlement.

Du ciblage (article 3 § 2 ; considérant 23 et 24) :

- Traitement des données personnelles de résidents de l'Union effectué par une entreprise basée en Suisse dans la mesure où elle traite ces données pour leurs **offres de biens et de services** dans l'Union, qu'un paiement soit exigé ou non (art. 3 § 2 (a) RGDP) ;

  Exemple 1 : une entreprise basée en Suisse vend des montres à des personnes domiciliées en France, Belgique, Portugal, Finlande et Grèce par le biais d'une boutique en ligne. Le RGPD est applicable car la société suisse offre des biens à des personnes dans l'Union.

[2] Le considérant 22 RGPD précise qu'un établissement suppose l'exercice d'une activité réelle et effective, au moyen d'un dispositif stable, et dans le cadre de l'activité de l'établissement. La forme juridique retenue pour un tel dispositif n'est pas déterminante à cet égard.
[3] La CNIL a rédigé un guide à l'attention des entreprises sous-traitantes qui continent notamment des exemples de clauses contractuelles de sous-traitance : https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants
[4] Pour autant que l'entreprise suisse ait l'intention d'offrir des biens ou des services à des résidents de l'Union européenne

Le RGPD n'offre pas de définition précise des notions d'offres de bien et de service. Le considérant 23 nous indique qu'il convient d'établir *«s'il est clair que le responsable du traitement ou le sous-traitant envisage d'offrir des services à des personnes concernées dans un ou plusieurs États membres de l'Union»*. Afin d'établir cette intention, il convient de prendre en compte un faisceau d'indices comprenant, par exemple: *«l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue, la mention de clients ou d'utilisateurs qui se trouvent dans l'Union »*.

Dans un contexte séparé (cf. Affaires jointes C-585/08 et C-144/09), la CJUE a déjà examiné la question de savoir si l'offre de biens et de services pouvait être considérée comme dirigée vers l'État membre de l'Union. Dans ce contexte, elle a également relevé les facteurs suivants : la mention d'un numéro de téléphone avec un indicatif téléphonique international, la description de l'itinéraire d'un État membre au lieu où le service est offert (ex. un hôtel suisse indiquant l'itinéraire à emprunter depuis l'étranger), la mention sur le site internet d'une clientèle internationale domiciliée dans divers États membres de l'Union, l'utilisation d'un domaine internet de premier niveau autre que celui de l'État membre où le service est offert (ex. le site www.exemple.ch sera également accessible sous www.exemple.fr et www.exemple.eu).

Cependant, *«la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention»*.

Il convient toutefois de souligner que tous ces facteurs cités ne sont pas exhaustifs et que la question devra toujours être analysée au cas par cas.

- Traitement des données personnelles de résidents de l'Union effectué par une entreprise basée en Suisse dans la mesure où elle traite ces données pour **le suivi du comportement** des personnes concernées au sein de l'Union (art. 3 § 2 (b) RGPD).

  En ce qui concerne la notion de suivi de comportement et de déterminer si une activité de traitement peut être considérée telle, le considérant 24 nous indique qu' *«il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit »*.

  Il s'agira notamment de la publicité comportementale qui, comme le défini le groupe de travail de l'Article 29 dans son avis sur la publicité comportementale, *«est une forme de publicité qui repose sur l'observation du comportement des individus au fil du temps. Elle vise à étudier les caractéristiques de ce comportement à travers leurs actions (visites successives de sites, interactions, mots clés, production de contenu en ligne, etc.) pour établir un profil spécifique et proposer aux personnes concernées des publicités adaptées à leurs centres d'intérêt ainsi déduits»*.

Exemple 2 : un hôtelier du val d'Hérens crée des profils de ses clients italiens, suédois, allemands et polonais afin de leur proposer des offres pour d'autres séjours, le RGPD sera applicable pour autant que le profil soit établi sur la base de comportement dans l'UE.

Exemple 3 : un exploitant de site web qui recourt au webtracking pour suivre les activités de ses visiteurs ou pour observer leur comportement de navigation pourra ainsi tirer des conclusions quant aux intérêts, préférences ou habitudes des internautes. Le RGPD sera sans doute applicable.

Obligations des entreprises concernées par le Règlement

L'une des grandes nouveautés par rapport à la Directive 95/46/CE est la consécration du principe de responsabilité («*accountability*») du responsable de traitement (cf. article 5 § 2 RGPD) en vertu duquel le responsable de traitement est **activement responsable de la mise en conformité** des traitements de données. Le responsable de traitement est responsable pour la conformité aux principes généraux et il doit également être capable de démontrer cette conformité. C'est sur la base de ce principe qu'a été dégagé le principe du **renversement du fardeau de la preuve**. Le Règlement prévoit notamment les obligations suivantes :

- L'article 24 RGPD souligne que le principe de responsabilité va de pair avec l'approche basée sur le risque selon laquelle le responsable du traitement va désormais devoir apprécier de façon objective la probabilité et le degré de risque encouru pour les droits et libertés des individus lorsqu'il entame un traitement. Le responsable de traitement devra ainsi mettre en place des mécanismes et des systèmes de contrôle au sein de son entité pour garantir la conformité du traitement pendant toute sa durée et pour en conserver la preuve.

- L'article 25 RGPD introduit les **principes de la protection des données dès la conception et protection des données par défaut**. Ils imposent que des garanties en matière de protection des données soient intégrées aux produits et services dès la phase initiale de leur conception.

- L'article 30 RGPD prévoit que chaque responsable du traitement ou son représentant devra tenir un **registre des activités de traitement** (sous forme électronique) effectuées sous leur responsabilité. Le contenu du registre est détaillé à l'article 30 § 1 RGPD. Ce registre devra être mis à disposition de l'autorité de protection des données lorsqu'elle le demande. Sauf exceptions, les entreprises de moins de 250 employés n'y seront pas soumises (cf. art. 30 § 5 RGPD).

- L'article 35 du RGPD prévoit la conduite d'une **analyse d'impact** sur la protection des données lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées[5]. Dans les cas où cette analyse préalable conduit à identifier des risques particuliers, le responsable sera tenu de consulter l'autorité de contrôle indépendante avant

[5] Pour accompagner les responsables de traitement dans leurs analyses d'impact sur la protection des données, la CNIL met à disposition un logiciel libre PIA sur son site internet : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil . La CNIL a également révisé ses "guides PIA" pour prendre en compte les nouveautés apportées par le RGPD et pour compléter son outil PIA distribué : https://www.cnil.fr/fr/nouveautes-sur-le-pia-guides-outil-piaf-etude-de-cas

la mise en œuvre du traitement ; si un délégué à la protection des données a été désigné, le responsable du traitement sera tenu de le consulter. Dans certains cas précis, l'analyse d'impact sera obligatoire (cf. art. 35 § 3) et le contenu minimum d'une telle étude est décrit à l'article 35 § 7.

La **sécurité des traitements** a été érigée en principe de base de la protection des données dans le Règlement :

- L'article 32 RGPD oblige le responsable du traitement à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque[6]. Ce faisant, il doit tenir compte 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 pour les droits et libertés des personnes physiques. À titre d'exemples, le Règlement cite entre autre la pseudonymisation, le chiffrement et des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes. En outre, le responsable du traitement doit prendre des mesures pour *«garantir que toute personne physique agissant sous son autorité, 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»* (cf. article 32 § 4).

De cette obligation de sécurité découle **l'obligation nouvelle de notifier à l'autorité de contrôle les violations** de données à caractère personnel. Dans certains cas, cette violation devra également être communiquée à la personne concernée :

- L'article 33 RGPD crée un système de notification des violations de données à caractère personnel[7] (*«data breaches»*). Cette notion de violation est défini comme *«une 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»* à l'article 4. 12 RGPD. En cas de violation susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, le responsable du traitement devra la notifier à l'autorité de contrôle dans les meilleurs délais et, si possible, 72 heures au plus tard (cf. article 33 § 1). Le sous-traitant doit quant à lui informer le responsable de toute violation de données sans retard injustifié après en avoir pris connaissance. Le contenu de la définition est prévu par l'article 33 § 3 RGPD. Enfin, le responsable de traitement doit conserver une **trace documentée de chaque violation** indiquant son contexte, ses effets et les mesures prises pour y remédier. Cette documentation doit permettre aux autorités de contrôle de mettre en œuvre leurs missions et pouvoirs.

- L'article 34 RGPD quant à lui prévoit les modalités et conditions applicables à la communication d'une brèche de sécurité aux personnes concernées. Aucun délai n'est en revanche prévu. L'idée sous-jacente est de permettre aux personnes concernée de prendre le cas échéant les

[6] Pour aider les professionnels dans la mise en conformité au RGPD, la CNIL a mis à jour son guide sur la sécurité des données personnelles : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

[7] L'autorité luxembourgeoise de protection des données a mis en ligne une page dédiée aux notifications de sécurité et qui comprend un formulaire téléchargeable : https://cnpd.public.lu/fr/declarer/violation-de-donnees/violation-donnees-rgpd.html

mesures qui s'imposent afin de faire cesser ou atténuer les effets négatifs pouvant découler de la violation des données

Dans trois cas précis (cf. article 37 RGPD), la **désignation d'un délégué à la protection des données** est rendue obligatoire[8]. C'est le cas pour : 1) les autorités publiques ou organisme publique, 2) les entreprises qui effectuent des traitements qui exigent un suivi régulier et systématique à grande échelle des personnes concernées 3) les entreprises qui effectuent des traitements de données sensibles. De plus, le Règlement permet au droit de l'Union ou au droit d'un État membre d'exiger la désignation d'un délégué à la protection des données dans des cas supplémentaires à ceux prévus par le RGDP. Un groupe d'entreprise peut également nommer un délégué unique ; cette possibilité existe aussi pour les autorités et entités publiques en tenant compte de la structure de leur organisation et de leur taille (article 37 § 2 et 3). Les qualités que le délégué à la protection des données doit posséder sont déterminées par l'article 37 § 5.

Finalement, le Règlement encourage l'élaboration de **codes de conduites** (art. 40 et 41 RGPD) destinés à contribuer à la bonne application du Règlement. Ils devront être élaborés en fonction de la spécificité des différents secteurs de traitement des données et des besoins spécifiques des entreprises. Ces codes seront soumis à l'autorité de protection des données compétente au titre de l'article 55 RGPD qui rendra un avis sur la conformité au Règlement. Les articles 42 et suivants mettent en place un **mécanisme de certification** permettant de venir en aide aux responsables et sous-traitants tenus de se conformer à des règles de protection.

Obligation de désigner un représentant des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union (art. 27 RGPD)

En cas d'application de l'article 3 § 2 RGPD, l'article 27 RGPD oblige les responsable du traitement mais aussi le sous-traitant qui ne sont pas établis dans l'Union à y désigner par écrit un représentant, lorsque le Règlement s'applique à leurs activités de traitement. Ce représentant doit être établi dans l'un des États membres dans lesquels résident les personnes physiques dont les données à caractère personnel sont traitées dans le contexte de l'offre de biens ou de services qui leur est proposée ou dont le comportement est observé (art. 27 § 3).

Selon le considérant 80 du RGPD, le représentant constitue notamment l'interlocuteur des autorités de contrôle (cf. article 58 RGPD) et les personnes concernées, sur toutes les questions relatives au traitement de données à caractère personnel. Ce dernier devra établir un **registre** de toutes les catégories d'activités de traitement de données à caractère personnel mises en œuvre sous sa responsabilité (cf. article 30 RGPD). Il pourrait également faire l'objet de procédures coercitives en cas de non-respect du présent règlement par le responsable du traitement ou le sous-traitant. Il est toutefois important de souligner que cela ne modifie en rien la responsabilité du responsable du traitement ou du sous-traitant à l'égard des autorités et des personnes concernées puisque cette désignation est sans préjudice d'actions en justice qui pourraient être intentées contre les responsable du traitement et sous-traitant eux-mêmes.

[8] Cf. Schéma «dois-je désigner un dpd »

L'article 27 § 2 précise que ce devoir de désignation ne s'applique pas :

a) « à un traitement qui est occasionnel, qui n'implique pas un traitement à grande échelle des catégories particulières de données visées à l'article 9, paragraphe 1, ou un traitement de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10, 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; ou

b) à une autorité publique ou à un organisme public.»

Sanctions prévues

Le Règlement, contrairement au droit suisse, reconnait le pouvoir aux autorités de contrôle d'imposer elles-mêmes des **amendes administratives** lorsqu'un certain nombre de conditions sont réunies. Chaque autorité de contrôle devra veiller à ce que les amendes administratives imposées pour des violations du RGPD soient **effectives, proportionnées et dissuasives**. Il ne faut, en effet, pas oublier que le Règlement met à disposition tout un éventail de moyens dissuasifs (cf. article 58 § 2 RGPD) comme l'avertissement, la mise en demeure, la limitation temporaire ou définitive d'un traitement et les rappels à l'ordre. Parmi tous ces outils, les autorités de protection des données devront choisir l'outil qui sera le plus à même d'atteindre l'objectif de mise en conformité.

Ce n'est donc qu'en ultime recours que les responsables d'un traitement peuvent s'exposer à des amendes d'un montant maximal de 20 millions d'euros ou correspondant à 4 % de leur chiffre d'affaires annuel mondial. L'article 83 RGPD liste les facteurs à prendre en compte pour fixer le montant de la sanction.

Il ne faut toutefois pas perdre de vue qu'il conviendra, le cas échéant, également de payer les éventuels dommages et intérêts des préjudices subis suite à un recours en justice.

À qui s'adresser :

Dans la mesure où le Règlement est un acte juridique européen, nous vous conseillons d'adresser vos questions concernant son application à une autorité de protection des données européenne comme la CNIL, la CPVP belge ou encore la CNDP luxembourgeoise. Nous vous recommandons également de consulter leurs sites internet qui contiennent des guides pratiques, des feuillets thématiques ainsi que des outils pratiques de conformité au Règlement