Application du Règlement Général sur la Protection des Données à la Réassurance

1. Introduction

1.1. Objectifs de la note

Cette note est issue d'un travail collaboratif des membres de la Commission Protection des données de l'APREF[1]. Cette note a pour objet d'aider à la mise en place du Règlement Européen au vu de la particularité des activités de réassurance.

Elle ne constitue en aucun cas un code de bonne conduite au sens de la réglementation en vigueur, ou un code de conduite au sens du Règlement Européen.

[1] APREF : Association des Professionnels de la Réassurance en France

1.2. Executive summary

Principaux objectifs du Règlement Général sur la Protection des Données personnelles (RGPD)
Le RGDP, entré en vigueur le 25 mai 2018, s'articule principalement autour de 4 objectifs :

- ➔ Harmoniser les législations européennes qui étaient jusqu'alors disparates ;
- ➔ Renforcer la protection et la gouvernance des données personnelles des résidents de l'Union Européenne ;
- ➔ Responsabiliser l'ensemble des personnes morales opérant un traitement de données personnelles ;
- ➔ Garantir les droits et libertés des personnes physiques.

Principaux changements résultant du RGPD
Le RGPD est, en France, moins une révolution qu'une évolution substantielle de la réglementation sur la protection des données personnelles, en y apportant notamment les modifications suivantes:

- ➔ **Principe de « Privacy by design »** : L'impératif de protection des données doit désormais être pris en compte dès la conception du traitement et tout au long de la vie de celui-ci;
- ➔ **Principe de « Privacy by default »** : Il s'agit de garantir, par défaut, du plus haut niveau possible de protection des données, grâce aux mesures techniques et organisationnelles appropriées et ce, de manière continue ;
- ➔ **Principe d' « Accountability »** : Tout réassureur doit être en mesure de démontrer aux autorités de contrôle qu'il est en conformité avec le RGPD (traçabilité et preuve du respect de chaque obligation). Il doit notamment à ce titre tenir un registre des activités de traitement qu'il exerce ;
- ➔ **Création de nouveaux droits** au profit des personnes physiques (droit à la limitation ; droit à la portabilité ; droit à l'oubli) avec un délai de réponse réduit;
- ➔ **Notification et la communication rapide de violations de données,** respectivement auprès de la CNIL et des personnes concernées ;
- ➔ **Obligation de procéder à une analyse d'impact des traitements** susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes protégées ;
- ➔ **Renforcement des sanctions** : Les sanctions pécuniaires sont dissuasives (jusqu'à 2% à 4% du chiffre d'affaire mondial consolidé, ou jusqu'à 10 à 20 M€, selon la gravité du manquement constaté) ;
- ➔ **Contrôle de la sous-traitance** : la sous-traitance est davantage règlementée. Elle doit notamment faire l'objet d'un contrat dont le contenu est règlementé en matière de protection des données ;
- ➔ **Suppression des obligations déclaratives** auprès de l'autorité de la CNIL (traitement, transferts hors UE) ;
- ➔ **Obligation de désigner un Délégué à la Protection des Données (DPD)** pour les réassureurs (suppression du Correspondant Informatique et Libertés-CIL).

Points d'attention

- ➔ Une bonne application du RGPD implique nécessairement la détermination des rôles, responsabilités et de la qualification juridique du réassureur, du courtier de réassurance et de ses partenaires. Il est indispensable de déterminer si le réassureur agit en qualité de responsable de traitement (le cas le plus fréquent), de responsable conjoint ou de sous-traitant ;
- ➔ L'obtention du consentement auprès de la personne concernée par le traitement de données pose des difficultés pratiques pour les réassureurs qui ne collectent jamais directement les données personnelles des assurés ou des tiers victimes ;
- ➔ Les délais imposés au titre des obligations de notification et de communication en cas de violation de données sont extrêmement courts. Il semble donc important d'anticiper ce risque et d'adapter sa capacité à y répondre ;
- ➔ La mise en place d'un registre de traitement n'est pas obligatoire pour tous les acteurs, mais elle est en tout état de cause vivement conseillée, le réassureur devant être en mesure d'apporter, à tout moment, la preuve de sa conformité à la réglementation.

1.3. Structure de la note

Le Règlement général sur la protection des données personnelles (RGDP) est entré en vigueur le 25 mai 2018.

Ce règlement s'applique à l'ensemble des traitements de données à caractère personnel **(2)** réalisés dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant sur le territoire de l'Union Européenne ainsi que les traitements relatifs à des personnes concernées se trouvant sur le territoire de l'Union Européenne.

Parce que le RGPD impose des obligations spécifiques aux sous-traitants dont la responsabilité peut être engagée en cas de manquement avéré, la détermination des rôles de responsable de traitement et de sous-traitant est essentielle **(3)**. A cet égard, le RGPD procède à un renversement de la charge de la preuve, car partant d'un système initial de déclaration et d'autorisation, avec contrôle de la conformité par la CNIL, c'est désormais au responsable de traitement ou au sous-traitant de prouver à tout moment sa conformité à la réglementation externe et interne en matière de protection des données à caractère personnel.

Par ailleurs, le responsable de traitement et le sous-traitant peuvent être contraints de désigner un Délégué à la Protection des Données (DPD) qui sera chargé de mettre en œuvre la conformité au RGPD au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme **(5)**.

A ce titre, le DPD sera notamment en charge de conseiller le responsable de traitement sur la nécessité ou non de réaliser pour les différents traitements de données personnelles une analyse d'impact relative à la protection des données **(4 et annexe2)**.

Cependant, il est à noter que le RGPD ne modifie pas toutes les dispositions du droit français actuellement applicable à la protection des données. Il en est ainsi de l'encadrement du transfert des données hors de l'Union Européenne **(6)**.

Enfin, la loi relative à la protection des données personnelles a été promulguée le 20 juin 2018. Elle reprend notamment les montants de sanctions que la CNIL pourra prononcer en cas de manquement aux obligations relatives à la protection des données. Dans un objectif de responsabilisation du responsable de traitement et du sous-traitant, le montant de ces sanctions a considérablement augmenté et peut aller jusqu'à 4% du chiffre d'affaires mondial ou vingt millions d'euros[2].

Un tableau comparatif des différents instruments législatifs en vigueur ou à venir se trouve en annexe de la présente note.

[2] La description complète de ces sanctions est visée en annexe 1 de la présente note.

Table des Matières

2. Données à caractère personnel, données sensibles et champ d'application

2.1.1. Définition des données à caractère personnel

Les données à caractère personnel sont définies à l'article 4 du RGPD.

Il s'agit de toute information professionnelle ou privée se rapportant soit à une personne physique identifiée, soit à une personne physique qui peut être identifiée directement ou indirectement par référence à un identifiant. Dans le second cas, les données peuvent être des données directement identifiantes (nom et prénom, numéro d'identification, photo ou vidéo, e-mail nominatif, etc…), des données indirectement identifiantes (NIR, empreinte digitale, domicile, données de localisation, etc…) ou le recoupement d'informations anonymes (le fils du coutier habitant au 11, bd Raspail à Paris).

En pratique, les données traitées par un réassureur dans son activité de réassurance sont les données des assurés et des tiers-victimes ainsi que les données de ses interlocuteurs chez les cédantes, les courtiers et les autres réassureurs ou rétrocessionnaires.

Le traitement de ces données, dès lors qu'elles entrent dans la définition des données à caractère personnel, doit se faire en conformité avec les dispositions du RGPD.

2.1.2. Définition des données sensibles

Les données sensibles constituent une sous-catégorie de données à caractère personnelles. Elles comprennent toutes les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques (ajouts du RGPD) et les données concernant la santé, la vie sexuelle ou l'orientation sexuelle.

Le traitement de données sensibles est en principe interdit. Elles peuvent néanmoins être traitées si les conditions suivantes sont remplies (ici les conditions rencontrées par un réassureur dans son activité de réassurance) :

- la personne concernée a donné son consentement explicite au traitement ;
- les données ont été manifestement rendues publiques par la personne concernée ;
- le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- le traitement est nécessaire pour des motifs d'intérêt public important (assurances obligatoires notamment) ;
- les données sont anonymisées à bref délai selon un procédé agréé par la CNIL (ajout de la loi Informatique et Libertés II).

2.1.3. Champ d'application

Le champ d'application matériel est inchangé par rapport à celui de la loi du 6 janvier 1978.

Il concerne les traitements de données personnelles, automatisés en tout ou partie, ainsi que les traitements non automatisés de données personnelles contenues ou appelées à figurer dans un fichier.

En revanche, le champ d'application territorial est élargi. Il concerne désormais les traitements réalisés dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant sur le territoire de l'Union Européenne ainsi que les traitements relatifs à des personnes concernées se trouvant sur le territoire de l'Union Européenne.

3. Le Réassureur, responsable de traitement ou sous- traitant?

3.1.1. Définitions

- Un responsable de traitement est celui qui « *seul ou conjointement avec d'autres**, déterminer les finalités et les moyens** du traitement [...]*[3]» ; et
- Le sous-traitant est celui qui « ***traite des données à caractère personnel pour le compte du responsable du traitement***[4] »

Il est important de rappeler que le terme de Sous-traitant au sens du RGPD ne doit pas être confondu, par exemple, avec celui de sous-traitant dans un contexte d'externalisation d'activité ou de fonctions critiques, lié à Solvabilité 2.

3.1.2. Critères de détermination et leur application à la réassurance

Afin de déterminer le statut, un faisceau d'indices, listés par la CNIL, dans son Guide du Sous-traitant publié en septembre 2017[5], doivent être pris en compte.

[3] *Article 4 (7) du RGPD*
[4] *Article 4 (8) du RGDP*
[5] https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf qui mentionne l'avis 1/2010 sur la notion de « Responsable de traitements et « Sous-traitant » du Groupe de travail « Article 29 »

- Autonomie : Le responsable de traitement est celui qui détermine, **en toute autonomie**, les finalités et les moyens d'un traitement. Le responsable de traitement est celui qui prend les décisions, sans se les voir imposer par une contrepartie extérieure, quant à la finalité qui justifie le traitement des données personnelles ainsi que les moyens avec lesquels elles sont traitées.

- Surveillance : Quel degré de contrôle et d'influence est exercé par la contrepartie sur les finalités poursuivis et les moyens utilisés pour le traitement des données personnelles ? Le degré de contrôle sera bien plus important dans le cadre d'une relation entre un responsable de traitement et son sous-traitant qu'entre deux Responsables de traitement.

- Transparence : l'identité du prestataire qui traite des données personnelles est-elle connue des personnes concernées ?

Dans le cadre d'une relation classique d'un traité de réassurance entre un assureur et un réassureur, le réassureur prend ses propres décisions, en toute autonomie afin de déterminer sa propre exposition au risque (le réassureur décidera, par exemple si le risque proposé est conforme ou non aux risques qu'il souhaite couvrir), de gérer ses engagements dans le cadre de règlement de sinistres. En effet, le réassureur traitera des données personnelles dans le but de mener ses propres analyses actuarielles, d'évaluation de sinistres que ce soit lors de négociations commerciales ou au cours de la vie d'un traité d'une manière que seul le réassureur détermine en toute autonomie. Lorsqu'il traite des données personnelles dans le cadre d'un traité de réassurance, le réassureur n'agit pas pour le compte de l'assureur ni sur ses instructions, il prend des décisions au regard de sa propre situation.

S'agissant du courtier de réassurance, qui est le mandataire de la cédante, il réalise des opérations de courtage entre la cédante et le réassureur. Compte tenu des critères visés ci-dessus, il semble que le courtier soit un responsable de traitement et non un sous-traitant de la cédante. En effet, le courtier ne traite pas les données personnelles des assurés transmises par la cédante pour le compte de cette dernière, mais les traite en toute autonomie car il détermine la finalité et les moyens du traitement au regard de sa propre activité, et communique ces données à tel ou tel réassureur lorsqu'il l'estime nécessaire.

Comme précédemment mentionné, être identifié comme responsable de traitement pour certains traitements de données personnelles, ne signifie pas qu'une entité ne peut pas agir en tant que sous-traitant pour d'autres traitements. Un courtier pourrait être considéré comme sous-traitant dans certains cas spécifiques en fonction de l'étendue du mandat. L'analyse est à faire au cas par cas.

3.1.3. Les obligations du responsable de traitement

En tant que responsable de traitement, le réassureur doit donc se conformer avec un certain nombre d'obligations qui s'articulent autour de 2 grands axes déterminés par l'Article 24 du RGPD :

- « Mise en œuvre de mesures techniques et organisationnelles appropriées » : un responsable de traitement se doit d'allouer des moyens suffisants et adéquats afin de répondre aux obligations qui pèsent sur lui dans le cadre des traitements de données personnelles qu'il réalise et des différents traitements qui peuvent être réalisés dans le cadre de son activité. Certaines de ces obligations ont été renforcées ou détaillées par le RGPD telles que les principes applicables aux traitements de données personnelles, les droits des personnes concernées auxquels le responsable de traitement doit être en mesure de répondre.

- Documenter afin de pouvoir prouver la mise en œuvre de ces mesures techniques et organisationnelles mentionnées ci-dessus. Il s'agit là l'un des grands changements apportés par le RGPD : on passe d'un contrôle à priori avec des autorisations préalables délivrées par la CNIL à celle d'un contrôle à postériori où le responsable de traitement comme le sous-traitant doivent être en mesure de prouver leur conformité à leurs obligations respectives. Il devient donc crucial de documenter les différents process, mesures de sécurité… afin de prouver cette « mise en œuvre de mesures techniques et organisationnelles. » Pour cela, le RGPD fait explicitement mention de la mise en place de polices ou de code de conduite qui sont dès lors considérés comme nécessaires afin que l'entité puisse démontrer être en conformité avec ses obligations.

3.1.4. L'exigence du consentement appliqué à la réassurance

Un élément central permettant la licéité de la collecte et du traitement de données personnelles porte sur le fait d'obtenir le consentement obtenu de la personne concernée (sauf autres cas de licéité figurant à l'annexe 4 – Tableau comparatif qui rendent le traitement régulier). L'obligation de démontrer que le consentement a correctement été obtenu est clairement attribuée au responsable de traitement[6].

Pour autant, le réassureur ne collecte pas directement les données personnelles des assurés couverts par le traité de réassurance, ces données sont collectées puis transférées par l'assureur. Cependant, le RDGP prévoit la situation où un responsable de traitement n'a pas directement collecté le consentement des données personnelles qu'il a à traiter : la conséquence principale en est qu'un certain nombre d'informations

[6] Article 7 du RGPD

supplémentaires doivent être fournies à la personne concernée.[7] Il existe cependant un certain nombre d'exemptions libérant le responsable de traitement de cette obligation d'information.

Le niveau de consentement requis est différent selon le type de données personnelles. Le recueil des données sensibles (voir 2.1.1) nécessite un « consentement **explicite**[8] » alors que pour les autres données personnelles, les personnes concernées doivent « simplement » consentir à leur traitement.

3.1.5. Sécurité des données à caractère personnel

Aux termes de l'article 32 du RGPD, le responsable de traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées aux fins de garantir un niveau de sécurité adapté au risque.

Parmi les mesures précitées, le RGPD prévoit une procédure de test et d'analyse de l'efficacité des systèmes de sécurité du traitement.

Si malgré la mise en place de ces mesures, une violation des données à caractère personnel survient, les articles 33 et 34 du RGPD imposent au responsable de traitement :

- **une notification de ladite violation auprès de l'Autorité de contrôle compétente (CNIL)** dans les 72 heures au plus tard après en avoir pris connaissance. Cette notification comprend :
    - une description détaillée de la violation des données et des conséquences probables de celle-ci ;
    - une communication du nom et des coordonnées du Délégué à la protection des données ;
    - une description des mesures prises ou que le responsable de traitement se propose de prendre pour remédier à la violation des données et le cas échéant en atténuer les conséquences.

  Le responsable de traitement accompagne la notification d'une documentation relatant les faits, leurs effets et les mesures prises pour y remédier.

- [*Si la violation s'avère susceptible d'engendrer un risque élevé pour les droit et libertés d'une/de personne(s) physique(s)*] **une communication de cette violation aux personnes concernées** dans les meilleurs délais. Cette communication comprend :
    - Une information en des termes clairs et simples quant à la nature de la violation de données et les conséquences probables de celle-ci;

[7] Article 14 du RGPD
[8] Article 9.2 a) du RGPD

- Une communication du nom et des coordonnées du Délégué à la protection des données ;
- une description des mesures prises ou que le responsable de traitement de propose de prendre pour remédier à la violation des données et le cas échéant en atténuer les conséquences.

Toutefois cette communication n'est plus nécessaire si :

- le responsable de traitement a mis en œuvre des mesures rendant les données incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès (Code / cryptage …) ;
- le responsable de traitement a ultérieurement pris des mesures garantissant que le risque n'est plus susceptible de se matérialiser ;
- cette mesure exigerait des efforts disproportionnés. Dans ce cas, le RGPD avance l'idée d'une communication publique (ou d'une mesure similaire).

Il est précisé que l'autorité de contrôle peut imposer au responsable de traitement cette communication si elle la juge opportune.

4. L'Analyse d'impact relative à la protection des données

Exemple révélateur de la philosophie du RGPD[9], l'analyse d'impact relative à la protection des données (AIPD) est un processus[10] dont l'objectif est double. D'une part, une analyse d'impact relative à la protection des données tend à décrire le traitement de données à caractère personnel envisagé, d'en évaluer la nécessité ainsi que la proportionnalité ; d'autre part, elle a vocation à aider à gérer les risques[11] pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face.

[9] Michael Bittan, *GDPR, le challenge des entreprises*, Introduction, p. 4, Deloitte, février 2018

[10] Pour plus de détails, les étapes de la réalisation d'une AIPD sont mentionnées en Annexe 1 de la présente note

[11] Conformément au Considérant 84 du RGPD, cette gestion des risques s'articule autour de trois axes :

- Établir le contexte : « compte tenu de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque » ;
- Apprécier le risque : « évaluer en particulier […] la probabilité et la gravité particulières du risque élevé » ;
- Traiter le risque : « atténuer ce risque », « assurer la protection des données à caractère personnel », et « démontrer le respect du […] Règlement. »

4.1.1. Les traitements concernés

L'article 35 du RGPD pose l'obligation de réaliser une AIPD « *lorsqu'**un** traitement […] est **susceptible d'engendrer un risque élevé pour les droits et libertés de la personne concernée*.* »

Le RGPD envisage trois hypothèses dans lesquelles il conviendra pour le responsable de traitement d'effectuer une AIPD :

- En cas d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, 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;
- En cas de traitement à grande échelle[12] de catégories particulières de données visées à l'article 9, paragraphe 1 (les données sensibles), ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10;
- En cas de surveillance systématique à grande échelle d'une zone accessible au public ».

Au-delà de ces trois hypothèses, le G29 préconise et conseille à tout responsable de traitement de prendre en compte la présence d'au moins un des critères suivants afin de déterminer et juger de l'opportunité de réaliser une étude d'impact sur la vie privée :

- L'évaluation ou la notation ;
- La prise de décisions automatisées avec effet juridique ou effet similaire significatif ;
- La présence de données sensibles ou données à caractère hautement personnel (art. 9 et art. 10 du RGPD) ;
- Le croisement ou la combinaison d'ensembles de données ;
- Le traitement de données concernant des personnes vulnérables : enfants, employés, personnes nécessitant une protection particulière (ex : patients) ;
- L'utilisation innovante ou l'application de nouvelles solutions technologiques ou organisationnelles qui pourrait impliquer de nouvelles formes de collecte et d'utilisation des données (exemple : impact sur la protection des données d'un produit technologique tel que les emails sécurisés) ;

[12] *Comment déterminer un traitement à grande échelle ?* Au regard du nombre de personnes concernées, soit en valeur absolue, soit en proportion de la population considérée; au regard du volume de données et/ou de l'éventail des différents éléments de données traitées; au regard de la durée ou la permanence de l'activité de traitement de données; au regard de l'étendue géographique de l'activité de traitement.

- Les traitements qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

4.1.2. Quels sont les traitements pour lesquels il est sûr qu'une analyse d'impact relative à la protection des données ne sera pas obligatoire ?

Trois hypothèses doivent ici être mentionnées :

- Tout d'abord, lorsque le traitement ne présente pas de risque élevé pour les droits et libertés de la personne concernée ;
- Ensuite, lorsque la nature, portée, le contexte et la finalité du traitement sont similaires à un traitement pour lequel une étude d'impact sur la vie privée a d'ores et déjà été menée ;
- Enfin, lorsque le traitement répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public, sous condition ; lorsque le traitement constitue l'une des exceptions prévues par la CNIL.

5. Le Délégué à la Protection des Données (DPD)

5.1.1. La désignation d'un DPD

5.1.1.1. Désignation obligatoire

L'article 37, paragraphe 1, du RGPD requiert la désignation d'un DPD dans trois cas spécifiques :

- lorsque le traitement est effectué par une autorité publique ou un organisme public;
- lorsque les activités de base[13] du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique[14] à grande échelle des personnes concernées; ou

[13] Les «activités de base» ne doivent pas être interprétées comme excluant les activités pour lesquelles le traitement de données fait partie intégrante de l'activité du responsable du traitement ou du sous-traitant. Par exemple, l'activité de base d'un assureur est de couvrir les assurés contre des risques identifiés (accident, maladie, décès, incendie, DDE..). Cependant, une société d'assurance ne pourra pas assurer la couverture de ces risques sans traiter des données concernant la personne ou les biens de l'assuré. Selon les lignes directrices du G29, dans ce cas, le traitement de ces données doit être considéré comme l'une des activités de base de la société d'assurance qui est donc dans l'obligation de désigner un DPD. Le même raisonnement s'applique aux activités de réassurance.

[14] Le profilage et notation à des fins d'évaluation des risques (par exemple, aux fins de l'évaluation du risque de crédit, de l'établissement des primes d'assurance, de la prévention de la fraude ou de la détection du blanchiment d'argent) est cité comme exemples d'activités pouvant constituer un suivi régulier et systématique des personnes concernées.

- lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Il est à noter que le traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités est directement cité en exemple dans les lignes directrices du G29 comme étant un traitement «à grande échelle».

En conséquence, **assureurs et réassureurs (s'ils traitent des données sur les assurés ou les tiers victimes) sont dans l'obligation de désigné un DPD**.

5.1.1.2. Désignation volontaire

Lorsqu'un organisme désigne un DPD sur une base volontaire, les conditions prévues aux articles 37 à 39 s'appliquent à la désignation, à la fonction et aux missions de celui-ci comme si la désignation avait été obligatoire.

5.1.2. Choix du pays de localisation du DPD

Le RGPD ne prévoit pas de dispositions spécifiques quant à la localisation du DPD. Néanmoins, le RGPD prévoit expressément que celui-ci soit joignable. En conséquence le G29 recommande que le DPD se trouve dans l'Union européenne et ce même si le responsable du traitement ou le sous-traitant sont établis en dehors de l'Union européenne[15]

5.1.3. Missions:

Les missions du DPD sont visées à l'article 39 du RGPD. Ainsi le DPD est tenu :

- D'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 RGPD et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;
- de contrôler le respect du RGPD, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données 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, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;
- de dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35;

[15] Lignes directrices concernant les délégués à la protection des données (DPD) adoptées le 13 décembre 2016. Version révisée et adoptée le 5 avril 2017

- de coopérer avec l'autorité de contrôle;
- de faire office de point de contact pour l'autorité de contrôle et de coopérer avec elle.

A noter que l'article 30 du RGPD impose l'obligation, pour le responsable de traitement ou le sous-traitant de tenir «*un registre des activités de traitement effectuées sous [sa] responsabilité» ou «un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement*». Néanmoins, il leur est possible de déléguer cette mission auprès du DPD.

5.1.4. Moyens mis à disposition du DPD

L'article 38 paragraphe 2 du RGPD prévoit expressément que le responsable du traitement et le sous-traitant "*aident le délégué à la protection des données à exercer les missions visées à l'article 39 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées*".

Les ressources mise à disposition du DPD varieront à la fois selon la nature des opérations et activités de traitement mais également de la taille de l'organisme concerné.

6. Transfert de données à caractère personnel hors UE

Le transfert est règlementé par le chapitre V du RGPD dont les dispositions s'appliquent :

- Aux transferts intervenant depuis l'Union Européenne vers un pays tiers ou à une organisation internationale ;
- Aux transferts ultérieurs à l'opération précitée, intervenant entre deux pays tiers à l'UE.

6.1.1. Transfert vers un pays dont la protection est jugée adéquat

Les transferts vers des pays tiers ou Organisations Internationales (OI) dont le niveau de protection a été jugé adéquat par la Commission européenne, peuvent avoir lieu sans autorisation préalable.

6.1.2. Transfert de données vers un pays qui n'est pas reconnu par l'UE comme bénéficiant d'une protection adéquate

Jusqu'à présent, de tels transferts étaient obligatoirement soumis à une autorisation préalable.
Désormais, le responsable de traitement ou le sous-traitant peut effectuer un tel transfert sans autorisation s'il justifie de garanties appropriées qui peuvent prendre la forme soit :

- d'un instrument juridiquement contraignant et exécutoire entre les autorités et organismes publics
- de règles d'entreprises contraignantes (ce corps de règles doit toutefois recueillir l'approbation préalable de l'autorité de contrôle de l'établissement qui les édicte)
- de clauses types de protection des données adoptées par la commission (
- de clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission;
- un code de conduite
- un mécanisme de certification approuvé conformément à l'article 42 du RGPD

6.1.3. Dérogations au principe d'interdiction des transferts (article 49)

Par ailleurs, en dehors des cas précités ci-dessus le RGPD reprend également les dérogations au principe d'interdiction des transferts qui étaient déjà prévues par la directive 95/46 Ce du 24 octobre 1995, et à l'article 69 de la loi Informatique et Libertés du 6 janvier 1978 (dont la liste se trouve en Annexe 3 de la présente note).

Le deuxième alinéa du 1 de l'article 49 prévoit une ultime possibilité de transfert. Toutefois cette exception est limitée à des cas ponctuels et exceptionnels et ne doivent pas concerner des transferts répétitifs, massifs ou structurels de données personnelles.

Contributeurs à la rédaction :

- Cécile Koczan, HANNOVER Re
- Eloïse Sorin, SCOR
- Arnaud Verrey, CCR
- Julien Vigeoz, XL CATLIN
- Guillaume Lachaud, SWISS RE

7. Annexe 1 Sanctions en cas de manquement aux obligations issues du RGPD

L'article 83 du RGPD[16] décrit les sanctions applicables au niveau communautaire pour les scinder selon deux degrés de gravité :

- **20.000.000,00 d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires mondial** total de l'exercice précédent (le montant le plus élevé étant retenu) en cas de violation :
  - des obligations résultant des principes de base d'un traitement (articles 5,6,7,9) ;
  - des droits dont bénéficient les personnes concernées (articles 12 à 22) ;
  - des transferts vers un pays tiers à l'UE (articles 44 à 49) ;
  - d'une violation de la législation des états membres relative à des situations particulières de traitement adoptée conformément au chapitre 9 du RGPD;
  - du droit d'accès, 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.

- **10.000.000,00 d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires mondial** total de l'exercice précédent (le montant le plus élevé étant retenu) en cas de violation (seules sont ici visées les sanctions applicables au responsable de traitement et au sous-traitant) :
  - Des conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information (article 8) ;
  - Des obligations relatives au traitement ne nécessitant pas l'identification la personne concernée (article 11) ;
  - Des principes de « *privacy by design* » et « *privacy by default* » (article 25)
  - Des dispositions relatives à la mission du délégué à la protection des données (article 39)
  - Des obligations pesant sur le responsable de traitement ou le sous-traitant en cas de certification (articles 42 et 43)

En tout état de cause, le montant des amendes prononcé variera en fonctions de divers critères d'appréciation énumérés à l'article 83.

En cas de violation de 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 peut pas excéder le montant fixé pour la violation la plus grave.

Les Etats membres peuvent également prévoir d'autres sanctions, pour les obligations dont la violation n'est pas expressément sanctionnée par le RGPD, conformément à l'article 84 du RGPD.

[16] Ces montants sont également repris par le projet de loi relatif à la protection des données personnelles adopté par l'AN le 13/02

Du reste, responsables de traitement et sous-traitants mettent en jeu leurs responsabilités à l'égard de toute personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD (article 82).

8. Annexe 2 – La réalisation de l'AIDP

Toute AIDP doit être effectuée « *avant le traitement* ». Cette exigence est cohérente avec les principes de protection des données dès la conception (Privacy by design) et de protection des données par défaut (Privacy by default).

Le G29 considère qu'il faut *a minima* respecter quatre étapes, prévues et décrite à l'Annexe 2 des lignes directrices susmentionnées, dans la réalisation d'une étude d'impact sur la vie privée :

- Première étape, délimiter et décrire le contexte du traitement envisagé - « *description systématique des opérations de traitement* » ;
- Deuxième étape, analyser les mesures garantissant le respect des principes fondamentaux - « *évaluation de la nécessité et de la proportionnalité des opérations de traitement* » ;
- Troisième étape, apprécier les risques liés à la vie privée par rapport à la sécurité des données - « *évaluation des risques pour les droits et libertés des personnes concernées* » ;
- Quatrième étape, formaliser la validation de l'étude d'impact sur la vie privée - « *mesures envisagées pour faire face aux risques* » et *a fortiori* « *apporter la preuve du respect du règlement* ».

Le RGPD ne fait pas obligation de publier l'AIPD, et il relève de la discrétion du responsable du traitement de la publier ou non. Cependant, le G29 considère qu'une « *publication au moins partielle, sous la forme d'un résumé ou d'une conclusion de son AIPD, devrait être envisagée par le responsable du traitement.* » Dans une telle hypothèse alors, la version publiée pourrait « *consister simplement en un résumé des principales constatations de l'étude d'impact de la vie privée, ou même uniquement en une déclaration selon laquelle une telle étude a été effectuée.* »

La CNIL considère quant à elle trois hypothèses dans lesquelles il conviendra de lui transmettre le rapport de l'étude d'impact sur la vie privée :

- Lorsque le risque résiduel reste élevé[17] : le responsable du traitement est tenu de se tourner vers l'autorité de contrôle pour une consultation préalable concernant le traitement (article 36, paragraphe 1). L'étude doit alors être communiquée dans son intégralité ;
- Lorsque la législation nationale l'exige ou en cas de contrôle de la CNIL.

[17] Un risque résiduel peut notamment être considéré comme élevé et inacceptable dès lors qu'il exposerait les personnes à des conséquences importantes, voire irréversibles, qu'elles seraient susceptibles de ne pas pouvoir surmonter (par ex.: un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière) et/ou lorsqu'il semble évident que le risque se concrétisera (par ex.: dans la mesure où il n'est pas possible de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée).

9. Annexe 3 : Dérogation au principe d'interdiction des transferts de données hors UE pour des situations particulières.

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:

- La personne concernée a donné son consentement explicite suite à une information relative aux risques résultant de ce transfert ;
- 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 ;
- Le transfert est nécessaire pour des motifs « importants » d'intérêt public ;
- Le transfert est nécessaire à la constatation, l'exercice ou la défense de droits en justice ;
- Le transfert et nécessaire à la sauvegarde d'intérêts vitaux de la personne concernée et celle-ci est dans l'incapacité physique ou juridique de donner son consentement ;
- 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.

Par ailleurs, si un transfert ne répond à aucun des cas précités, l'article 49 du RGPD (2ème partie) prévoit une ultime possibilité de transfert lorsque :

- ce transfert ne revêt pas de caractère répétitif ;
- ne touche qu'un nombre limité de personnes concernées ;
- 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 ;
- le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel ;
- Le responsable du traitement informe l'autorité de contrôle du transfert. Outre qu'il fournit les informations visées aux articles 13 et 14, le responsable du traitement informe la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.

10. Annexe 4 Tableau comparatif

Catégories	Sous-catégories (art./Règlement UE)	Loi Informatique et Libertés	Règlement UE	Loi sur la protection des données personnelles du 20 juin 2018
Les définitions	Définitions (article 4)	- Données à caractère personnel - Traitement - Fichier - Responsable de traitement - Sous-traitant	Idem	
	Définitions (article 4)		- Profilage - Pseudonymisation - Destinataire (interne et externe) - Violation de données personnelles - Données génétiques et biométriques (nouvelles données sensibles) - Responsables conjoints d'un traitement	
Les traitements	Champ d'application matériel (art. 2)	Application au : - traitement de données personnelles, automatisé en tout ou partie - traitement non automatisé de données personnelles contenues ou appelées à figurer dans un fichier	Idem	
	Champ d'application territorial (art. 3)	Application au traitement : - dont le responsable est établi sur le territoire français - dont le responsable, sans être dans un Etat de l'UE, recourt à des moyens de traitements situés sur le territoire français	Application au traitement : - réalisé dans le cadre des activités d'un établissement d'un responsable de traitement / sous-traitant sur le territoire de l'UE - relatif à des personnes concernées se trouvant sur le territoire de l'UE	

Les traitements	Qualité des données (article 5)	- traitée de manière licite, loyale et transparente - adéquates, pertinentes et limitées au regard de la finalité du traitement - exactes et, si nécessaire, tenues à jour	Idem	
	Finalité du traitement (art.5)	Données collectées pour des finalités déterminées, explicites et légitimes, et traitées après de manière compatible avec ces finalités	Idem	
	Durée de conservation (art.5)	Conservation des données à caractère personnel pendant une durée n'excédant pas celle nécessaire au regard de la finalité du traitement	Idem	
	Licéité du traitement (art. 6)	Consentement de la personne concernée ou autres conditions : - le respect d'une obligation légale - l'exécution d'un contrat auquel la personne concernée est partie - l'exécution d'une mission d'intérêt public - les intérêts légitimes poursuivis par le responsable du traitement	Consentement libre, spécifique, éclairée et univoque de la personne concernée ou autres conditions (idem) Consentement valide de l'enfant de + de 16 ans	Consentement valide de l'enfant de + de 15 ans Consentement éclairé et exprès de la personne concernée à obtenir avant traitement de ses caractéristiques génétiques
	Privacy by design (art.25)		Mesures garantissant la prise en compte des exigences réglementaires dès la conception du traitement	
	Privacy by default (art.25)	Données limitées au regard de la finalité du traitement	Mesures garantissant que, par défaut, seules les données nécessaires à la finalité du traitement sont traitées	
	Sous-traitance choix (article 28)		- sous-traitant présentant des garanties suffisantes - pas de recrutement par le sous-traitant d'un autre sous-traitant sans l'accord préalable du responsable de traitement	Sous-traitants exclus du champ d'application du Règlement UE soumis à la loi Informatique et Libertés II (article 35)
	Sous-traitance contrat (article 28)	Contrat avec le sous-traitant doit prévoir des obligations de sécurité et de confidentialité à sa charge portant sur données fournies	Contrat obligatoire avec le sous-traitant doit prévoir des obligations supplémentaires à sa charge	
	Registre des activités de traitements (art.30)	Registre des activités de traitement avec rubriques obligatoires (si désignation d'un CIL)	Registre des activités de traitement avec nouvelles rubriques obligatoires (sauf si entreprises - de 250 salariés ou traitement de données sensibles ou condamnations pénales)	

Les données sensibles où à risque élevé	Traitements Données sensibles (article 9)	Interdiction sauf exceptions	Idem (sauf retrait de l'exception pour les données anonymisées à bref délai)	Retour de l'exception pour les données anonymisées à bref délai Conformité des traitements de données de santé à un référentiel méthodologique de la CNIL (sauf exceptions)
	Analyse d'impact Conditions (art.35)		Si le traitement engendre un risque élevé pour les droits et libertés des personnes physiques (exemple : traitement à grande échelle de données sensibles)	Analyse d'impact non requise pour : - Les traitements qui ont des finalités de statistiques publiques, mis en œuvre par le service statistique public et ne comportant aucune des données mentionnées au I de l'article 8 (catégories particulières de données) ou à l'article 9 (données relatives aux infractions et condamnations) – conditions cumulatives ; - Les traitements qui ont des finalités de recherches scientifiques ou historique ; - Les traitements qui mettent à la disposition des usagers de l'administration un ou plusieurs télé services de l'administration électronique (ordonnance n°2005-1516 du 8 décembre 2005, art. 1er) mis en œuvre par l'État ou une personne morale de droit public ou une personne morale de droit privé gérant un service public.
	Analyse d'impact Analyse (art.35)		- Description systématique des opérations de traitement envisagées et des finalités du traitement - Evaluation de la nécessité des opérations de traitement au regard des finalités - Evaluation des risques pour les droits et libertés des personnes concernées - Mesures envisagées pour faire face aux risques	
	Analyse d'impact Consultation préalable de la CNIL (art.36)		Cas : l'analyse d'impact indique que le traitement présenter un risque élevé même si le responsable prend pas de mesures pour atténuer ce risque	
Transfert vers pays hors UE	Décision d'adéquation (article 45)	Autorisation préalable si décision d'adéquation ou non	Plus d'autorisation préalable si décision d'adéquation	

Transfert vers pays hors UE	Transferts autorisés si garanties appropriées (article 46)	Autorisation préalable quand transferts vers pays hors de l'UE ou à réglementation équivalente avec: - Clauses types de protection des données - Règles d'entreprise contraignantes	Plus d'autorisation préalable si garanties appropriées	

Catégories	**Sous-catégories** (art./Règlement UE)	**Loi Informatique et Libertés**	**Règlement UE**	**Loi sur la protection des données personnelles du 20 juin 2018**
La gouvernance	Mesures techniques et opérationnelles (art.24)		Principe : mesures appropriées pour s'assurer et être en mesure de démontrer que les traitements sont conformes au règlement, à actualiser si nécessaire	
	Mesures techniques et opérationnelles Contrôle et Audit (art.24)		Application : mise en œuvre de politiques appropriées (dont contrôles à plusieurs niveaux)	
	Mesures techniques et opérationnelles Documentation (art.24)		Application : mise en place d'une documentation permettant de démontrer que les traitements sont conformes au règlement	
	Sécurité des traitements Principe (art.32)	Préservation de la sécurité des données pour empêcher qu'elles soient déformées, endommagées ou accessibles à des tiers non autorisés	Selon la nature du traitement, mise en œuvre des mesures appropriées pour garantir un niveau de sécurité adapté au risque sur les droits et libertés des personnes concernées	
	Sécurité des traitements Mesures (art.32)	Sécurité logique et physique des traitements	- Pseudonymisation ou chiffrement des données - Moyens garantissant l'intégrité, la confidentialité, la disponibilité et la résilience des traitements - Moyens permettant le rétablissement des données dans des délai appropriés en cas d'incidents - Procédure de tests avec évaluation de l'efficacité de la sécurité des données	

La gouvernance	DPO - Désignation (art. 37 et 38)	Facultative	Obligatoire si : - autorité publique ou organisme public - activités de base : profilage - activités de base : traitement à grande échelle de données sensibles	
	DPO missions antérieures (art. 39)	- Consultation sur toute question relative à I&L - Point de contact de la CNIL - Information et conseil - Contrôle du respect de la réglementation interne et externe - Tenue du registre des traitements	Idem	
	DPO nouvelles missions (art. 39)		- Assemble et actualise la documentation et les preuves sur la conformité - Notifie les violations de données à la CNIL - Veille au respect des engagements contractuels sur la protection des données - Vérifie l'exécution des études d'impact	
	Sanctions CNIL (art.83)	Jusqu'en 2016 : maximum 300 000 € Depuis 2016 : maximum 3M€	Manquements les + graves : maxima 20 M€ ou 4% du CA mondial Autres manquements : maxima 10 M€ ou 2% du CA mondial	
Les personnes concernées	Informations - collecte directe (art.13)	Informations à donner à la personne concernée lors de la collecte	Informations complémentaires à donner à la personne concernée lors de la collecte	
	Informations- collecte indirecte (art.14)	Informations à donner à la personne concernée lors de leur enregistrement	Informations complémentaires à donner à la personne concernée dans un délai raisonnable et sous un mois	
	Droits de la personne concernée (art.15)	- droit d'accès - droit de rectification - droit d'opposition - droit à l'effacement	Nouveaux droits : - droit à la limitation - droit à la portabilité - droit à l'oubli	
	Droits de la personne concernée (art.15)	Délai de réponse de deux mois. Possibilité de s'opposer à une demande abusive	Délai de réponse d'un mois	

Les personnes concernées	Notification violation CNIL (art.33)		Notification dans les 72h de la violation de données accidentelle ou illicite engendrant un risque sur droits ou libertés d'une personne quand : - destruction, altération ou divulgation - accès non autorisé	
	Communication violation personnes concernées (art.34)			Décret en Conseil d'Etat à venir : liste des traitements autorisés à déroger à l'obligation de communiquer à la personne concernée la violation de ses données lorsque la notification d'une divulgation ou d'un accès non autorisé à ces données est susceptible de représenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique
	Violation de données Dispense (art.33 et 34)		En cas de mesures appropriées rendant les données incompréhensibles à un tiers (chiffrement)	
	Formation et sensibilisation du personnel (art. 39 et 47)		Sensibilisation et formation appropriée en matière de protection des données pour le personnel ayant un accès permanent ou régulier aux données	