Décider devient facile.

Le Règlement général sur la protection des données

Le livre blanc des experts SVP

Pourquoi vous proposer un livre blanc sur le Règlement UE relatif à la protection et au traitement des données à caractère personnel ?

La question du traitement des données à caractère personnel apparaît comme un enjeu économique majeur. La quantité de données collectées augmente chaque année et sera au cœur de l'économie de demain.

Le nouveau Règlement général sur la protection des données, dit RGPD, du 27 avril 2016, applicable à partir du 25 mai 2018 par l'ensemble des pays membres de l'Union européenne (UE), prévoit un principe d'auto-responsabilisation des acteurs économiques.

Les entreprises et les personnes publiques doivent, dès à présent, se mettre en conformité, créer les outils adaptés et mettre en place des processus de collecte en adéquation avec le RGPD.

Au niveau national, la réglementation découlant de la loi informatique et liberté du 6 janvier 1978 avait déjà initié et familiarisé les acteurs économiques sur leurs obligations et les droits des personnes, avec la création de la *Commission national de l'informatique et des libertés* (CNIL).

Dans une volonté d'harmonisation, le RGPD uniformise la protection des données au sein de l'UE en abrogeant la directive 95/46/CE. Etant d'application directe, le RGPD détrône la loi informatique et liberté de 1978 et pose des questions d'adaptation.

Le RGPD énonce un nouveau principe de protection des données. Les acteurs économiques devront passer du système de la déclaration CNIL vers un système d'auto-responsabilité, avec la mise en place de la fonction de « *Délégué à la protection des données* » (DPD), appelée aussi « *Data Protection Officer* » (DPO). L'obligation de réaliser une cartographie des traitements et, le cas échéant, des études d'impact sont des fondamentaux de la nouvelle règlementation.

Le DPO sera un super CIL (*Correspondant informatique et liberté découlant de la loi de 1978*) dont la désignation sera obligatoire dans la majorité des cas, avec la possibilité d'avoir un DPO externe.

Le RGPD consolide les droits des personnes en introduisant des nouveautés comme le droit à l'oubli ou la portabilité des données personnelles et renforce les pouvoirs de l'autorité nationale de contrôle.

La CNIL, dans la continuité de ses prérogatives, verra avec le RGPD ses pouvoirs de sanction évoluer.

Dans ce livre blanc, les experts SVP mettent en avant les éléments prépondérants du RGPD ainsi que l'ensemble des droits et obligations des acteurs économiques.

Avertissement : Dans ce livre blanc sont principalement utilisés les termes ou acronymes les plus usités par les acteurs économiques. Une traduction ou définition de ceux-ci sont également présents.

Sommaire

1. Rappel des notions fondamentales prévues par le Règlement européen

Le Règlement européen relatif à la protection des données à caractère personnel s'applique au traitement, automatisé ou non, des données personnelles (articles 2 et 3 du Règlement) :

- Effectué dans le cadre des activités 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,
- Relatif à des personnes concernées qui se trouvent sur le territoire de l'Union, et ce même si le responsable de traitement ou le sous-traitant n'est pas établi sur le territoire de l'Union européenne dès lors que les activités de traitement sont :
    - liées 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

    - liées 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.
- Par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un Etat membre s'applique en vertu du droit international public (la Suisse par exemple).

a) Quelques définitions

- **Fichier**

Selon l'article 2 alinéa 4 de la loi informatique et libertés, « constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés ».

Et selon l'article 4 du Règlement : « tout 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 ».

- **Traitement**

La loi informatique et libertés de 1978 donne une définition très générale de ce qu'est un traitement. Au vu de cette dernière, tout le monde traite de la donnée. Le Règlement européen a repris une définition similaire.
Article 2, alinéa 3 de la loi informatique et libertés :

« Constitue un traitement de données à caractère personnel toute opération ou ensemble d'opérations portant sur de telles données quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

Article 4.2 du Règlement européen :

« Traitement, 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, 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 ».

Constitue un traitement de données personnelles, toute opération portant sur des données personnelles, quel que soit le procédé utilisé. Il s'agit aussi bien de l'enregistrement des données, de leur conservation ou encore de leur modification.

Par ailleurs, le traitement peut être informatisé ou non.

- **Données à caractère personnel**

L'article 4 du Règlement européen :

Il définit les données à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Cet article donne une définition très large : toutes données permettant d'identifier une personne physique (par exemple le nom et la date de naissance d'une personne). Les adresses IP, les cookies ou autres identifiants, ainsi que la voix sont également une donnée à caractère personnel.

b) Les différents acteurs

1) Le responsable de traitement

Le responsable de traitement est la personne, l'autorité publique, le service ou l'organisme qui détermine la finalité et les moyens du traitement.

En général, est responsable de traitement, la personne morale représentée par son représentant légal. Lorsque le responsable du traitement est situé en dehors du territoire français et plus largement en dehors de l'Union européenne, il doit désigner auprès de la CNIL un « représentant établi sur le territoire français » à moins que le traitement soit occasionnel, ou n'implique pas un traitement à grande échelle ou des données sensibles.
La jurisprudence du Conseil d'Etat du 12 mars 2014 sur la notion de responsable de traitement dans le cadre d'une société mère avec ses filiales retient que la société mère est responsable de traitement car elle a déterminé les finalités et les moyens du traitement, en ce qu'elle a décidé de la nature des données collectées, déterminé les droits d'accès à celles-ci, fixé la durée de conservation des données et apporté les correctifs nécessaires après le contrôle de la CNIL.

2) Le destinataire

La définition de destinataire change dans le cadre du nouveau Règlement européen.

Le destinataire est *« 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 Etat membre ne sont pas considérées comme des destinataires ».*

3) La personne concernée

La personne concernée est une notion très large qui vise notamment :

- La personne à laquelle se rapportent les données qui font l'objet du traitement ;

- Toute personne sur qui peut porter des données collectées ou des données qui font l'objet d'une opération de traitement.

4) Les sous-traitants

Selon l'article 4 du Règlement, il s'agit de « *toute personne traitant des données à caractère personnel pour le compte du responsable du traitement* ».

Sont donc considérées comme « sous-traitant », toutes les personnes physiques ou morales qui interviennent pour le compte du responsable du traitement, telles que les sociétés en charge de la conservation des données et les hébergeurs.

Si le traitement est réalisé par un sous-traitant pour le compte du responsable de traitement, ce dernier devra vérifier que son sous-traitant présente des garanties suffisantes en matière de sécurité et confidentialité, notamment en termes de connaissances spécialisées, de fiabilité et de ressources.

L'application d'un code de conduite approuvé ou d'un mécanisme de certification peut être un moyen de prouver le respect de ces obligations.

Le sous-traitant ne peut agir que sur instruction du responsable du traitement et les parties doivent conclure un contrat précisant, notamment, ce point et détaillant les obligations incombant au sous-traitant en termes de sécurité et de confidentialité.

Le responsable du traitement a toujours pour obligation de veiller au respect de ces mesures même s'il fait appel à un sous-traitant.

Le Règlement européen instaure une co-responsabilité entre le responsable de traitement et le sous-traitant.

En effet, l'article 82 du Règlement dispose que 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.

Le sous-traitant est tenu pour responsable du dommage causé par le traitement :

- S'il n'a pas respecté les obligations prévues par le présent Règlement qui incombent spécifiquement aux sous-traitants ;

- S'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

En cas de procédure judiciaire, le Règlement prévoit que « *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* ».

c) Les principes relatifs au traitement des données à caractère personnel

Plusieurs principes sont présents dans le Règlement :

- Licéité, loyauté, transparence : les données doivent être « *traitées de manière licite, loyale et transparente au regard de la personne concernée* » ;

- Limitation des finalités : les données doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités » ;

- Exactitude des données : les données doivent être exactes et, si nécessaire, tenues à jour ;

- Limitation de la conservation des données : les données doivent être *« 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 »* ;

- Intégrité et confidentialité (l'article 34 de la loi informatique et libertés) les données doivent être *« 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 »*.

1) Licéité du traitement

Pour pouvoir être réalisé, le traitement doit être licite, c'est-à-dire qu'il doit remplir l'une, au moins, des conditions fixées à l'article 6 du Règlement :

- *« la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;*
- *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 ;*
- *le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;*
- *le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;*
- *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 ;*
- *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* ».

2) Licéité du traitement

Il existe certaines catégories de données pour lesquelles le traitement est en principe interdit, sauf dérogation spécifique. Il s'agit du « *traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* » (article 9).

Le Règlement européen laisse une marge de manœuvre aux pays concernant les catégories particulières de données à caractère personnel en leur permettant de prévoir des dérogations spécifiques notamment :

- les traitements pour lesquels la personne concernée a donné son consentement exprès pour une ou plusieurs finalités spécifiques ;
- les traitements nécessaires à la sauvegarde de la vie humaine ;
- les traitements portant sur des données rendues publiques par la personne concernée ;
- les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- les traitements nécessaires pour des motifs d'intérêt public important.

Les traitements sensibles sont ceux :

- portant sur des données biométriques ;
- portant sur des données génétiques ;
- portant sur les infractions, condamnations et mesures de sûreté ;
- portant sur les numéros de Sécurité sociale ;
- comportant des appréciations sur les difficultés sociales des personnes ;
- ayant pour objet l'interconnexion de fichiers ;
- etant susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire (création de « blacklist ») : il s'agit par exemple d'une liste des personnes avec lesquelles l'entreprise ne veut plus contracter. Dans le cadre de ces « listes noires », la personne concernée doit être informée et elle ne peut figurer indéfiniment sur la blacklist.

2. Le principe de responsabilisation : « accountability »

Le Règlement met en place une logique de responsabilisation du responsable de traitement qui devra pouvoir justifier auprès de l'autorité de contrôle qu'il a bien pris toutes les mesures nécessaires pour que les données qu'il collecte et traite soient correctement protégées.

a) Qu'est-ce que l'« accountability » ?

Le responsable de traitement va devoir prouver qu'il se conforme bien à ses obligations en matière de protection des données à caractère personnel et que toutes les mesures appropriées afin de protéger efficacement les données collectées ont bien été prises.

Cela peut se faire par :

- ✓ la tenue d'un registre reprenant les activités de traitement des données (art 30) ;
- ✓ la réalisation d'études d'impact sur la vie privée (EIVP ou PIA) ;
- ✓ la mise en place de mesures nécessaires à la sécurité et la confidentialité des données comme la tenue d'un registre ou la notification des failles de sécurité ;
- ✓ la nomination d'un délégué à la protection des données (DPO) et une coopération avec l'autorité de contrôle ;
- ✓ l'application d'un code de bonne conduite approuvé notamment par l'autorité de contrôle et comprenant les mécanismes permettant de procéder au contrôle obligatoire du respect de ses dispositions par les responsables du traitement ou les sous-traitants qui s'engagent à l'appliquer (art 24 et 40).

Le corollaire est un allégement des formalités administratives.

Les obligations déclaratives ne seront plus nécessaires dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Cette volonté de responsabilisation va conduire, de ce fait, à un allégement des formalités administratives.

b) La protection des données personnelles dès la conception d'un service et par défaut : Privacy by design ou by default (article 25)

Le responsable de traitement doit veiller à ce que toute application, produit ou service traitant des données à caractère personnel offre dès leur conception le plus haut niveau possible de protection des données.

Il se doit également de garantir cette protection « par défaut », ce qui signifie que les paramètres de confidentialité les plus stricts s'appliquent automatiquement une fois qu'un client acquiert un nouveau produit ou service.

Afin de respecter ces principes, des systèmes d'information et des traitements conformes doivent être conçus *ab initio*.

Pour cela, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation (le traitement de données à caractère personnel doit être réalisé de telle façon que les données ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires), afin de protéger les droits des personnes concernées et 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, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes sans l'intervention de la personne physique concernée.

3. La mise en place d'outils pour garantir une protection optimale des données collectées et traitées

L'entreprise doit porter une attention particulière à ce que seules soient collectées et traitées, les données strictement nécessaires à la poursuite de ses objectifs et être vigilante à ce que leur protection soit assurée. Pour ce faire, elle devra prendre des mesures afin de garantir la protection des données, par le biais d'une cartographie des traitements et de la tenue d'une documentation interne spécifique, et pourra (et parfois même devra) désigner une personne qui aura pour mission de conseiller l'entreprise, de contrôler le respect de la protection des données personnelles et qui servira d'interlocuteur avec l'autorité compétente.

a) Le délégué à la protection des données (DPO)

1. Obligation de désigner un DPO (article 37 RGPD)

Le responsable du traitement et le sous-traitant désignent en tout état de cause un DPO lorsque :

- le traitement est effectué par une autorité ou un organisme public (sauf fonction juridictionnelle) ;

- le traitement à caractère personnel implique un suivi régulier, systématique et à une échelle importante ;

- les activités consistent en un traitement à grande échelle de données sensibles (origine, génétique, infraction,…) ou des données relatives à des condamnations pénales et à des infractions.

Il n'y a pas de définition du traitement à « grande échelle » dans le RGPD, les membres du G29 (Groupe des autorités de protection européennes) recommandent de tenir compte de la quantité de données traitées, de la durée de conservation et de son étendue géographique. En dehors des cas de désignation obligatoire, la désignation du DPO est encouragée par les membres du G29.

Un groupe d'entreprise peut désigner et mutualiser le DPO, les coordonnées du DPO doivent être publiées pour permettre l'accessibilité du DPO à tous les acteurs du groupement.

2. Choix d'un DPO

Le DPO peut être interne (salarié) ou externe (prestataire de service), il devra être 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.

Le RGPD ne précise pas les conditions de qualification et de formation du DPO, il devra avoir une expertise juridique de la législation nationale et européenne sur la protection des données proportionnée à sa sphère de compétence et d'une formation continue. Le RGPD ne nous donne pas d'élément sur la durée des fonctions du DPO.

3. Fonctions du DPO

Les organismes doivent fournir à leur DPO les ressources nécessaires à ses missions, il doit être associé, d'une manière appropriée et en temps utile aux traitements de données. Il ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement.

Il sera soumis au secret et à une obligation de confidentialité.

Il convient de faire attention aux risques de conflits d'intérêts avec ses autres fonctions.

4. Missions du DPO

Ses prérogatives se sont renforcées. Il est chargé d'informer et conseiller le responsable du traitement, le sous-traitant et les employés qui procèdent au traitement sur leurs obligations et leurs droits. Il contrôle le respect du RGPD et des droits découlant du traitement et sera chargé de la coopération avec l'autorité de contrôle.

Le DPO doit tenir compte dans l'accomplissement de ses missions, des risques associés aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités de ce dernier.

5. Transition des fonctions de CIL vers les fonctions du DPO

Dans la continuité de l'application de la loi informatique et libertés du 6 janvier 1978 prévoyant la faculté de nomination d'un Correspondant informatique et libertés (CIL), le CIL devrait avoir la possibilité d'élargir ses fonctions en devenant DPO.

6. Comparaison entre les obligations du CIL et du DPO

CIL	DPO
Tenir la liste des traitements et assurer son accessibilité : tenue d'un registre.	La tenue du registre n'est plus dans les attributions du DPO sauf s'il y a une attribution par le biais d'une clause contractuelle.
Veille en toute indépendance au respect de la loi.	Contrôle le respect du RGPD et des droits découlant du traitement. Informe et conseille le responsable du traitement, le sous-traitant et les employés qui procèdent au traitement sur leurs obligations et leurs droits.
Fonction de médiation et de coordination, le CIL est chargé de recevoir les réclamations des personnes concernées par les traitements des données.	Les personnes concernées peuvent prendre contact avec le DPO 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 présent Règlement.
Le CIL établit annuellement un bilan de ses activités qu'il soumet au responsable du traitement et le transmet sur demande à la CNIL.	Cette mission n'est pas énumérée par le RGPD mais elle pourra être incluse dans le cadre de ses autres missions qui seront contractuellement prévues.
Les missions prévues pour le DPO ne sont pas exercées par le CIL aujourd'hui.	Le DPO devient le point de contact et doit coopérer avec l'autorité de contrôle.
	Dispense des conseils en ce qui concerne l'analyse d'impact et vérifie son exécution.
	Le DPO contrôle le respect des règles internes du responsable du traitement ou du sous-traitant, y compris sur la répartition des responsabilités, la sensibilisation et la formation du personnel.

b) La cartographie des traitements et études d'impact

Afin de se mettre en conformité avec le Règlement européen et pouvoir, notamment, tenir la documentation nécessaire à la bonne gestion des risques, chaque entreprise devra commencer par faire un inventaire des traitements des données à caractère personnel qu'elle collecte et / ou traite.

Une « cartographie des traitements » devra être réalisée et permettra d'identifier les actions à mener en interne pour être conforme au Règlement.

Par ailleurs, si lors de cet inventaire la société constate que les traitements effectués comportent des risques pour les droits et libertés des personnes, elle devra réaliser une analyse d'impact et, dans certains cas, consulter l'autorité compétente.

1. Cartographie des traitements

Pour parvenir à cartographier les traitements réalisés par la société, il sera d'abord nécessaire de recenser :

- les différents traitements de données personnelles mis en œuvre au sein de l'entreprise concernée ;
- le type de données personnelles traitées ;
- les objectifs poursuivis par le traitement ;
- les acteurs internes et externes (sous-traitants) qui s'occupent de ce traitement ;
- le lieu où les données collectées sont hébergées ;
- la durée de leur conservation ;
- les mesures de sécurité prises pour minimiser les risques ;
- ou encore le transfert des données, notamment hors Union européenne, s'il y a lieu.

⇨ *Identifier les actions à mener pour se conformer au Règlement*

Après avoir procédé à la cartographie des traitements des données, l'entreprise doit porter une attention particulière à ce que seules soient collectées et traitées les données strictement nécessaires à la poursuite de ses objectifs et être vigilante :

- au respect des modalités d'information prévues par le Règlement (informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée, informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée…) ;

- au respect des modalités d'exercice des droits des personnes concernées (accès, rectification, portabilité, suppression…) ;

- aux mesures de sécurité mises en place ;

- au respect de ses obligations par le sous-traitant (clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées).

2. Réalisation d'une étude d'impact relative à la protection des données pour les traitements à risque

Afin d'apprécier les risques sur la protection des données du point de vue des personnes concernées, la réalisation d'études d'impact (EIVP ou PIA : « Privacy Impact Assessment ») pourra s'avérer nécessaire.

En effet, si le traitement des données collectées ou traitées est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable de traitement doit réaliser, avant le traitement, une analyse d'impact sur la vie privée (article 35 du Règlement).

Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.
Dans ce cas, le responsable de traitement demandera conseil au DPO, s'il y en a un.

Cette étude d'impact va, notamment, permettre d'évaluer l'origine, la nature et la gravité du risque, principalement en raison du contexte et de la finalité du traitement, et de mettre en place un traitement de données personnelles respectueux de la vie privée.

Elle doit être réalisée préalablement à la collecte des données personnelles et à la mise en œuvre du traitement de ces dernières et devra comprendre, notamment, les mesures, les garanties et les mécanismes envisagés pour atténuer ce risque.

Si cette étude d'impact indique que le traitement présenterait un risque élevé et si le responsable de traitement ne peut pas prendre de mesures appropriées pour atténuer le risque en raison des techniques disponibles et des coûts de mise en œuvre, une consultation préalable de l'autorité de contrôle devra être effectuée (article 36).

L'article 35 précise les cas dans lesquels l'analyse d'impact est requise :

- ✓ *« 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 ;*

- ✓ *le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ; ou*

- ✓ *la surveillance systématique à grande échelle d'une zone accessible au public ».*

L'autorité de contrôle pourra établir et publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact est ou non requise.

Selon l'article 35 du Règlement, l'analyse d'impact contient a minima :

- *« une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;*

- *une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;*

- *une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et*

- *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 présent Règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées ».*

c) La tenue d'un registre des activités de traitement et d'une documentation interne

Le Règlement ayant pour but de responsabiliser les responsables de traitement, chaque société devra renforcer son dispositif contractuel, mettre en place une documentation interne et tenir également, dans certains cas, un registre des activités de traitement.

1. Mise en place d'un registre des activités de traitement (article 30)

Sauf exceptions (cf. ci-dessous), chaque responsable de traitement a l'obligation de tenir un registre des activités de traitement. Ce registre comporte les informations suivantes :

- ✓ 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 ;
- ✓ les responsables des services opérationnels traitant les données au sein de l'entreprise ;
- ✓ les sous-traitants ;
- ✓ les catégories de données traitées ;
- ✓ les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple, les données relatives à la santé) ;
- ✓ les finalités pour lesquelles les données sont collectées ou traitées (ex : RH, gestion clients…) ;
- ✓ une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- ✓ les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées ;
- ✓ le lieu où les données sont hébergées ou transférées et les documents attestant de l'existence de garanties appropriées ;
- ✓ les délais prévus pour l'effacement des différentes catégories de données (pendant combien de temps chaque catégorie de données est conservée) ;
- ✓ une description générale des mesures de sécurité mises en œuvre pour minimiser les risques d'accès non autorisés aux données.

En cas de sous-traitance, le sous-traitant tiendra un registre de toutes les activités de traitement effectuées pour le compte du responsable de traitement.

Ces registres se présentent sous une forme écrite, y compris la forme électronique, et doivent être tenus à la disposition de l'autorité de contrôle.

L'article 30 indique une exception à la tenue du registre : la tenue du registre des activités de traitement par le responsable de traitement et/ou par le sous-traitant ne s'impose pas à une « *entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions* ».

2. Constitution d'un dossier documentaire

Les entreprises doivent conserver un dossier :

- ✓ Comprenant la documentation relative aux traitements des données personnelles : le registre des traitements, quand il est obligatoire, les analyses d'impact réalisées, l'encadrement des transferts hors U.E notamment par le biais de BCR (Binding Corporate Rules / Règles internes de l'entreprise) ou de clauses contractuelles.

- ✓ Comprenant la documentation relative à l'information des personnes : les mentions d'information communiquées à la personne dont les données ont été collectées, le modèle du recueil du consentement des personnes, la procédure mise en place pour l'exercice du droit des personnes (droit d'accès, de modification...).

- ✓ Comprenant les contrats définissant les rôles et la responsabilité de chaque acteur : les contrats avec les sous-traitants, les procédures en cas de violation des données (registre).

La tenue d'une telle documentation permettra à la société de prouver, en cas de contrôle, qu'elle est bien en conformité avec le Règlement européen et qu'elle a pris toutes les mesures nécessaires pour respecter les droits des personnes dont les données personnelles ont été collectées et traitées.

d) La sécurité du traitement et déclaration des failles de sécurité

A partir de mai 2018, chaque organisme, entreprise ou personne publique devra mettre en place un processus de gestion des incidents de sécurité et aura l'obligation de notifier toute violation des données personnelles. L'obligation de sécurité était déjà présente à l'article 34 de la loi de 1978, mais le Règlement prévoit une obligation générale de sécurité renforcée qui passe notamment par l'obligation de notification des failles de sécurité.

Article 4 : « *violation de données à caractère personnel », 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* ».

1. Sécurité du traitement des données

Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques.

La sécurité du traitement, prévue à l'article 32 du Règlement, peut consister en :

- ✓ « *la pseudonymisation et le chiffrement des données à caractère personnel ;*

- ✓ *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;*

- ✓ *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 ;*

- ✓ *une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ».

2. Processus de gestion des failles de sécurité

Le gestionnaire du traitement devra formaliser les procédures de gestion des incidents et pourra s'inspirer du processus défini par la norme ISO/IEC 27035.

Cela implique, en amont de la survenance de l'incident, d'identifier les personnes, en interne et en externe, impliquées dans leur gestion. Il peut s'agir, de ce fait, des personnes en charge de la sécurité des systèmes d'information, de la protection des données personnelles, des prestataires de service externes, ainsi que des personnes à qui doivent être notifiées ces incidents. La liste de ces personnes devra être tenue à jour.

Un dispositif de veille devra techniquement être mis en place (fournisseurs, IRT (Incident Response Team)…), ainsi qu'un dispositif de détection et de remontée d'alertes (ce qui permet de détecter les activités anormales ou suspectes).

Après avoir réalisé l'évaluation des informations, il faudra déterminer si l'incident est avéré ou non, ainsi que les autorités devant être destinataires de la notification.

Si l'incident de sécurité n'entraîne aucun risque pour les personnes, il devra uniquement être reporté sur un registre dans lequel figurera également les mesures prises pour le résorber.

En revanche, si l'incident entraîne un risque pour les personnes, le responsable de traitement devra en notifier les autorités compétentes : la CNIL, mais également parfois l'ARS (Agence régionale de la santé).

La création d'un « arbre de décision » permettant d'identifier les différentes actions à mener pour chaque incident est préconisée.

- **Tenue d'un registre**

En cas de violation des données personnelles (telle que écrasement de fichiers, destruction, perte, altération, divulgation ou un accès non autorisé à des données personnelles, même de manière accidentelle), les faits, les effets et les mesures pour remédier à cette faille de sécurité devront être consignés dans un registre. La société devra donc « documenter l'incident ».

- **Notification**

Dès lors qu'un traitement de données à caractère personnel subit une atteinte sécuritaire entrainant un risque pour les personnes concernées, le responsable de traitement devra procéder à certaines notifications.

- Notification à la CNIL

L'entreprise doit notifier à la CNIL dans les 72h de la connaissance de la violation, exception faite si cette faille de sécurité n'est pas susceptible de porter atteinte aux droits et libertés des personnes concernées (art 33-1). Tout retard dans la notification devra être justifié. La notification peut se faire par étape si nécessaire (art 33-4).

Le contenu de la notification doit être précis, détaillé et documenté.

La notification doit contenir « à tout le moins » : des détails sur la nature de la violation et sur sa portée (types de données, nombre de personnes et d'enregistrements concernés), les coordonnées du DPO (Délégué à la Protection des Données), décrire les conséquences probables et les mesures pour les limiter ou y remédier.

Si la violation de données à caractère personnel n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques concernées, le responsable de traitement n'aura pas à informer la CNIL, mais la violation en question devra être consignée dans un registre tenu à disposition de celle-ci. Même si aucun formalisme n'est prévu pour ce registre, il faudra y faire figurer la date et les modalités de l'incident, ainsi que les mesures réalisées pour y remédier.

La CNIL devrait normalement mettre en place un système de téléservice pour recevoir les notifications.

La CNIL précise que devront être communiqués les éléments suivants :

- « *la description de la nature de la violation de données à caractère personnel ;*
- *les catégories de données ;*
- *le nombre approximatif de personnes concernées par la violation ;*
- *les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;*
- *le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues, de décrire les conséquences probables de la violation de données et enfin de préciser les mesures prises ou à 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* ».

- Notification des personnes concernées

En cas de risque élevé pour les droits et libertés des personnes, le responsable de traitement doit informer, en des termes clairs et simples, les personnes physiques concernées par l'indicent, et ce dans les meilleurs délais.

Toutefois, si le responsable de traitement a pris, préalablement ou postérieurement à la violation des données, des mesures techniques ou organisationnelles appropriées (par exemple si les données perdues sont illisibles du fait d'un cryptage), la notification ne sera pas nécessaire.

La CNIL précise que « *dans le cas où la communication aux personnes concernées exigerait des efforts disproportionnés, une communication publique ou autre mesure similaire tout aussi efficace peut être réalisée* ».

Elle pourra également, si elle l'estime nécessaire, demander au responsable de traitement ne l'ayant pas fait, d'effectuer cette communication.

En cas de sous-traitance, le sous-traitant a l'obligation d'informer, sans délai, le responsable de traitement des failles de sécurité dont il a connaissance (art 33-2).

Jusqu'à présent cette obligation de notification n'était réservée qu'aux fournisseurs d'accès Internet (FAI). Le Règlement généralise l'obligation de notification.

e) La mise en place technique et les certifications

1. Mise en place technique

Ainsi qu'il a été évoqué précédemment, l'article 32 du RGPD donne quelques pistes d'orientation pour la mise en place technique.

L'entreprise ou la collectivité pourra notamment protéger les données personnelles en les rendant anonymes et en procédant au chiffrement de celles-ci.

L'anonymisation ou le chiffrement des données suppose, bien évidemment, l'utilisation d'une solution informatique qui réalisera le travail au fil de l'eau et permettra aux seules personnes autorisées d'accéder aux informations pour lesquelles elles ont été habilitées par le DPO.

L'utilisation de moyens de protection de l'ensemble des accès, de type pare-feu par exemple, doit également être envisagée, si ceux-ci n'existent pas au préalable. Le Règlement précise que ces moyens doivent garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante du système d'information. L'obligation de résultat est donc bien précisée, le système de protection doit être d'une performance sans faille.

Il est également nécessaire de mettre en place un système d'information redondant, c'est-à-dire entièrement doublé. Le système dispose donc d'une installation jumelle distante, les données sont systématiquement copiées et mises à jour sur les deux systèmes. Ainsi, en cas d'indisponibilité temporaire ou définitive d'un des deux systèmes, le deuxième permet une remise en service rapide de l'ensemble des fonctionnalités.

Enfin, des procédures techniques et organisationnelles doivent être définies et mises en œuvre pour tester et évaluer, en permanence la sécurité du système et des données.
La formation de l'ensemble des utilisateurs est également un élément essentiel pour la sécurité des données. Les statistiques de la cybercriminalité montrent que les vols de données ont malheureusement souvent pour origine une erreur humaine. Le développement exponentiel de logiciels espions est une menace forte. Certains virus informatiques visent principalement les données personnelles, soit pour les dérober (cheval de Troie) ou les rendre inaccessibles sauf à verser une somme d'argent pour les récupérer (ransomware). Les codes de conduite doivent définir clairement l'utilisation des postes de travail et des moyens de communication pour éviter l'intrusion de pirates informatiques dans le système d'information.

2. Certifications et labels

Les articles 42 et 43 du RGPD prévoient des mécanismes de certification et de labels. Ces qualifications, délivrées par un organisme de certification disposant d'un niveau d'expertise approprié en matière de protection des données (CNIL, Comité européen ou entité extérieure accréditée) permettront de *« démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le RGPD »*.

La dernière version du référentiel pour la délivrance de labels en matière de procédures de gouvernance tendant à assurer la protection des données de la CNIL a été adoptée et publiée au JORF du 20 septembre 2017.

4. Le principe de transparence : information et consentement de la personne concernée

Le RGPD vient délimiter précisément les modalités d'information devant être respectées afin d'obtenir le consentement éclairé des personnes impactées par la collecte de données, ainsi que d'appréhender les droits découlant de la collecte de ces données.

a) L'information de la personne concernée

1) Informations à fournir au moment de la collecte (article 13)

- identité et coordonnées du responsable du traitement ;
- coordonnées du DPO ;
- finalités du traitement ainsi que la base juridique du traitement ;
- si collecte sur le fondement de l'article 6, I point F : information sur les intérêts légitimes de la collecte ;
- les destinataires ou les catégories de destinataires de la collecte ;
- la durée de conservation (ou si imprévisible : critère de fixation de la durée) ;
- informations sur le droit de la personne sur ses données collectées (accès, suppression, rectification, limitation….) ;
- le droit d'introduire une réclamation auprès de la CNIL ;
- sur le caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et sur les conséquences sur la non-fourniture des données ;
- sur l'existence d'une prise de décision automatisée ;
- si traitement ultérieur : information sur la nouvelle finalité.

Il n'est pas nécessaire de fournir les informations si la personne concernée dispose déjà de celles-ci.

2) Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée (article 14)

- informations similaires à celles prévues à l'article 13 ;
- si le responsable du traitement a l'intention d'effectuer un transfert des données à un destinataire dans un pays tiers ou à une organisation internationale et les garanties appropriées ;
- la source d'où proviennent les données (si source accessible ou non au public).

Le délai pour fournir ces informations :

- délai raisonnable après l'obtention des données à caractère personnel : maximum 1 mois ;
- si les données doivent être utilisées aux fins de communication avec la personne concernée : au plus tard au moment de la communication ;

- si les données sont destinées à un autre destinataire : au plus tard au moment la première communication.

Aucune information n'est nécessaire si :

- la personne concernée dispose déjà de ces informations ;
- la fourniture de telles informations se révèle impossible ou exigerait un effort disproportionné ;
- la collecte est prévue par la loi ;
- les données sont confidentielles (ex : obligation légale découlant du secret professionnel).

b) L'obtention du consentement

L'article 4 du Règlement définit le consentement comme *« 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 ».*

Pour traiter les données personnelles d'une personne, son consentement préalable doit toujours être obtenu, sauf en cas de :

- ✓ contrats et mesures précontractuelles : quand il s'agit d'une relation avec un client ou prospect (par exemple en créant un compte sur internet) ;
- ✓ obligation légale du responsable de traitement (ex : l'employeur) ;
- ✓ sauvegarde de la vie humaine ;
- ✓ mission de service public (ex : les impôts) ;
- ✓ intérêt légitime du responsable de traitement.

Le consentement doit être :

- ✓ libre (art 4) ;
- ✓ démontré : il faut garder une preuve du consentement (art 7-1). Il faut une traçabilité (ex : signature, empreinte vocale, code envoyé par téléphone…) ;
- ✓ retiré aussi facilement qu'il a été donné (art 7-3). Cela peut se faire par écrit (y compris voie électronique) ou par oral ;
- ✓ éclairé et univoque (art 11 et 40).

c) Les droits de la personne concernée

1) Droit d'accès

La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées, ainsi qu'un droit d'accès aux données.

- Même informations que l'article 14 ;
- Copie des données.

2) Droit de rectification (article 16)

La personne concernée a le droit à la rectification des données qui sont inexactes ou incomplètes dans les meilleurs délais.

3) Droit à l'effacement et à l'oubli (article 17)

Le droit à l'effacement dans les meilleurs délais s'applique si :

- les données personnelles ne sont plus nécessaires au regard de la finalité du traitement ;
- retraitement du consentement (conformément à l'article 6, I point F ou article 9, 2 point a) ;
- opposition au traitement en vertu de l'article 21 ;
- le traitement est illicite ;
- effacement afin de respecter une obligation légale ;
- les données personnelles sont collectées sur le fondement de l'article 8, 1 (sur le consentement des enfants) ;
- les données à caractère personnel ont été rendues publique et que le responsable du traitement est tenu de les effacer. Il doit prendre des mesures raisonnables y compris d'ordre technique, pour informer les tiers responsables du traitement sur cette demande d'effacement.

Il n'y a pas de droit à l'effacement dans les hypothèses suivantes :

- exercice du droit à la liberté d'expression et d'information ;
- pour respecter une obligation légale ;
- motifs d'intérêts publics ;
- à des fins archivistiques ;
- nécessaire à la constatation, à l'exercice ou à la défense en justice.

4) Droit à la limitation du traitement (article 18)

La personne concernée par le traitement peut obtenir la limitation du traitement si l'un des éléments suivants s'applique si :

- l'exactitude des données est contestée par la personne (le responsable du traitement dispose d'un délai de vérification) ;
- le traitement est illicite (limitation sauf si la personne souhaite l'effacement) ;
- les données ne sont plus nécessaires pour le responsable du traitement mais nécessaire pour la personne concernée pour la constatation, l'exercice ou la défense en justice (action en justice) ;
- l'opposition de la personne (article 21), 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.

5) Droit de notification (article 19)

Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation.

6) Portabilité (article 20)

- Droit d'obtenir les données dans un format structuré, couramment utilisé et lisible par une machine ;
-
- Droit de transférer les données directement auprès d'un nouveau responsable du traitement.

7) Droit d'opposition (article 21)

- La personne concernée peut s'opposer à tout moment, pour des raisons personnelles, au traitement de ses données y compris pour le profilage ;

- L'exercice du droit d'opposition implique que le responsable du traitement évalue le droit de la personne concernée au non traitement de ses données et les motifs légitimes du responsable du traitement de poursuivre ce traitement malgré cette opposition ;

- Le responsable du traitement doit informer la personne concernée de son droit d'opposition *« au plus tard au moment de la première communication avec la personne concernée »* ;

- Les personnes concernées peuvent s'opposer, mais il ne sera pas fait droit à leur demande d'opposition si le traitement est *« nécessaire à l'exécution d'une mission d'intérêt public »*.

8) Profilage (article 22)

- Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris du profilage, sauf si cela est :
  - *autorisé par la loi ;*
  - *« nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement » ;*
  - *fondé sur le consentement explicite de la personne.*

  Le responsable du traitement doit mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne.

5. Le transfert de données à caractère personnel vers des pays tiers ou vers des organisations internationales

Il peut arriver que les données collectées soient transférées vers des pays situés hors de l'Union européenne ou vers des organismes internationaux. Si tel est le cas, le responsable de traitement aura l'obligation d'informer la personne concernée du transfert de ses données, et de prendre certaines garanties afin d'en assurer la protection.

a) Le principe : interdiction du transfert des données personnelles hors Union européenne

Le transfert des données au sein de l'Union européenne n'est soumis à aucune restriction. En revanche, le transfert de données d'un pays de l'Union européenne vers un pays situé hors de l'Union (« flux transfrontières ») est par principe interdit.

b) Les exceptions

1) Transferts fondés vers un pays tiers ayant un niveau de protection adéquat (article 45 du Règlement et article 68 de la loi informatique et libertés)

Le transfert de données à caractère personnel vers un pays tiers ou vers une organisation internationale ne sera possible que si le pays destinataire des données a un niveau de protection des données personnelles suffisant et adéquat (exemple : Argentine, Canada, Suisse, Nouvelle-Zélande).

Le caractère suffisant du niveau de protection assuré par un Etat est apprécié par la Commission et « *s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées* ».

2) Transferts moyennant des garanties appropriées (article 46 du Règlement)

Si le pays destinataire n'a pas de protection suffisante, « *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 des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives* ».

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

- L'existence d'un accord négocié dans le pays en question,

Il peut exister des accords négociés dans certains pays et auxquels les entreprises nationales acceptent d'adhérer. Par exemple, existait aux USA le Safe Harbor Act remplacé par le Privacy Shield.

- La signature de clauses contractuelles entre les deux responsables de traitement ou un responsable de traitement et un sous-traitant,

La Commission européenne a adopté des clauses contractuelles types de contrats de transfert de données personnelles (décision 2001/497/CE du 15 juin 2001, modifiée par la décision du 24 décembre 2004).

- L'adoption de codes de bonne conduite (ou BCR),

Ces codes de bonne conduite sont des règles d'entreprises contraignantes (« Binding Corporate Rules » ou BCR) qui ont pour objectif de définir la politique d'un groupe en matière de transfert de données personnelles hors UE.

L'entreprise doit rédiger un projet de BCR qui devra être approuvé par l'autorité de contrôle compétente (la CNIL) qui, après avis, procédera à son enregistrement et à sa publication. Toute modification de ces règles d'entreprise devra être signalée à la CNIL.

Pour être approuvées, ces BCR doivent être juridiquement contraignantes, respectées par toutes les entreprises du groupe, y compris leurs employés ; elles doivent conférer expressément aux personnes concernées des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel et répondre à certaines exigences spécifiques prévues par le Règlement européen.

3) Autres dérogations pour des situations particulières

Le transfert vers un pays tiers ou une organisation internationale est possible :

- Si la personne à laquelle se rapportent les données a consenti expressément à leur transfert 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,

- si le transfert est nécessaire à l'une des conditions suivantes :

  - ✓ à la sauvegarde de la vie de cette personne ;

  - ✓ à la sauvegarde de l'intérêt public ;

  - ✓ au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;

  - ✓ à la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

  - ✓ à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;

  - ✓ à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

Avant tout transfert de données à caractère personnel vers un pays tiers (hors Union européenne) ou une organisation internationale, le responsable de traitement devra informer la personne concernée de son intention d'effectuer un tel transfert (article 13 du Règlement) et devra l'informer des garanties appropriées prises en ce qui concerne ce transfert.

L'information relative aux transferts des données devra également figurer dans le registre des activités de traitement pour toute entreprise ayant l'obligation d'en tenir (article 30 du Règlement) et dans les codes de conduite s'il en a été établi (article 40 du Règlement).

6. Les autorités de contrôle

La mise en place d'un droit unifié de protection des données à caractère personnel a nécessité la création d'une entité juridique indépendante chargée de l'application cohérente du RGPD avec un pouvoir de conseil. Au niveau national, chaque Etat membre doit créer une ou plusieurs autorités de contrôle avec des pouvoirs d'enquête et de sanction.

a) Le Comité européen

Le Comité européen de la protection des données est institué en tant qu'organe indépendant de l'Union disposant de la personnalité juridique.

Le Comité se compose du chef d'une autorité de contrôle de chaque Etat membre et du contrôleur européen de la protection des données, ou de leurs représentants respectifs.

⇨ Si plusieurs autorités de contrôle dans un Etat membre : désignation d'un représentant commun.

La Commission européenne a le droit de participer aux activités et réunions du Comité sans droit de vote, sauf lorsque les décisions concernent les principes et les règles applicables aux institutions, organes et organismes de l'UE.

1) Président du Comité et ses missions

Le Comité élit son président et deux vice-présidents en son sein à la majorité simple, pour un mandat de cinq ans renouvelable une fois.

Il sera chargé de :

- Convoquer les réunions du Comité et d'établir l'ordre du jour ;
- Notifier les décisions adoptées par le Comité à l'autorité de contrôle chef de file et aux autorités de contrôle concernées ;
- Veiller à l'accomplissement, dans les délais, des missions du Comité, notamment en ce qui concerne le mécanisme de contrôle de la cohérence.

Le Comité fixe dans son règlement intérieur la répartition des tâches entre le président et les vice-présidents.

2) Secrétariat

Le Comité dispose d'un secrétariat, qui est assuré par le Contrôleur européen de la protection des données.

3) Missions du Comité

Le Comité veille à l'application du RGPD notamment de :

- Surveiller et garantir la bonne application du RGPD dans les cas prévus dans sa mission d'avis et règlements des litiges ;
- Conseiller la Commission :
    - sur toutes questions relatives à la protection des données à caractère personnel dans l'Union ;
    - sur les règles d'entreprise contraignantes, 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.
- Publier des lignes directrices, des recommandations et des bonnes pratiques sur les 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 ;
- Examiner, de sa propre initiative, à la demande de l'un de ses membres ou à la demande de la Commission, et de publier des lignes directrices, des recommandations et des bonnes pratiques afin :
    - de favoriser l'application cohérente du RGPD ;
    - de préciser les critères et conditions applicables aux décisions fondées sur le profilage ;
    - de préciser les circonstances particulières dans lesquelles un responsable du traitement ou un sous-traitant est tenu de notifier la violation de données à caractère personnel ;
    - de préciser les circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'engendrer un risque élevé ;
    - de préciser davantage les 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 sur des règles d'entreprise contraignantes appliquées par les sous-traitants ;
    - d'élaborer, à l'intention des autorités de contrôle, des lignes directrices concernant l'application de leurs pouvoirs, ainsi que la fixation des amendes administratives.
    - de faire le bilan de l'application pratique des lignes directrices, recommandations et des bonnes pratiques ;

- d'établir des procédures communes pour le signalement par des personnes physiques de violations du RGPD ;

- 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 ;
- de procéder à l'agrément des organismes de certification et à l'examen périodique de cet agrément et de tenir un registre public des organismes agréés, ainsi que des responsables du traitement ou des sous-traitants agréés établis dans des pays tiers ;

- de rendre à la Commission un avis sur les exigences en matière de certification ;

- de rendre à la Commission un avis sur :

  - 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 ;

  - les projets de décisions des autorités de contrôle conformément au mécanisme de contrôle de la cohérence visé à l'article 64, paragraphe 1, sur les questions soumises et d'émettre des décisions contraignantes ;

  - les codes de conduite élaborés au niveau de l'UE.

- de promouvoir la coopération et l'échange bilatéral et multilatéral effectif d'informations et de bonnes pratiques entre les autorités de contrôle ;

- 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.

- Le Comité transmet ses avis, lignes directrices, recommandations et bonnes pratiques à la Commission, et les publie ;

  - Le Comité établit un rapport annuel sur la protection des personnes physiques à l'égard du traitement dans l'Union et, s'il y a lieu, dans les pays tiers et les organisations internationales. Le rapport est rendu public et contient le bilan de l'application pratique des lignes directrices, recommandations, bonnes pratiques et décisions contraignantes.

4) Procédure

Le Comité prend ses décisions à la majorité simple de ses membres, sauf disposition contraire du RGPD.

Le Comité adopte son règlement intérieur et ses modalités de fonctionnement.

b) La CNIL

1) Membres

Le RGPD prévoit que les membres doivent être nommés selon une procédure transparente par leur Parlement, leur gouvernement, leur chef d'Etat, ou un organisme indépendant.

La durée du mandat du ou des membres ne peut être inférieure à quatre ans, sauf pour le 1er mandat.

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 nomination échelonnée.

Le RGPD prévoit une autorité de contrôle, chef de file, et des autorités de contrôle spécifique.

Le mandat est renouvelable et le nombre de mandat est fixé par l'Etat membre :

- La CNIL comporte 18 membres :
    - 4 parlementaires (2 députés, 2 sénateurs) ;
    - 2 membres du Conseil économique, social et environnemental ;
    - 6 représentants des hautes juridictions (2 conseillers d'État, 2 conseillers à la Cour de Cassation, 2 conseillers à la Cour des comptes) ;
    - 5 personnalités qualifiées désignées par le Président de l'Assemblée nationale (1 personnalité), le Président du Sénat (1 personnalité), en Conseil des Ministres (3 personnalités) ;
    - 1 Commissaire du gouvernement.
- Le mandat des commissaires est de 5 ans ou, pour les parlementaires, d'une durée égale à leur mandat électif.

2) Missions (RGPD et loi 1978)

- Contrôle de l'application du RGPD ;

- Favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits ;

- Joue un rôle de conseil auprès de l'Etat ;

- Sensibilise les responsables du traitement ou sous-traitants sur leurs obligations ;

- Traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association ;

- Coopère avec les autres autorités de contrôle (partage d'informations, assistance mutuelle…) ;

- Effectue des enquêtes sur l'application du RGPD ;

- Suit le développement et les évolutions dans le domaine des technologies de l'information, de la communication et des pratiques commerciales ;

- Effectue une analyse d'impact relative à la protection des données ;

- Encourage la mise en place de mécanismes de certification ainsi que de labels → approuve les critères de certification ;

- Procède, à l'examen périodique des certifications délivrées ;

- Rédige et publie les critères d'agrément d'un organisme chargé du suivi des codes de conduite ;

- Procède à l'agrément d'un organisme chargé du suivi des codes de conduite ;

- Autorise les clauses contractuelles et les dispositions visées à l'article 46 paragraphe 3 ;

- Approuve les règles d'entreprise contraignantes ;

- Contribue aux activités du Comité ;

- Tient des registres internes des violations au présent règlement.

3) Coûts

L'accomplissement des missions de l'autorité de contrôle est gratuit pour la personne concernée sauf si les demandes sont manifestement infondées ou excessives.

4) Pouvoirs

- Pouvoir d'enquête :
    - Ordonner au responsable du traitement et au sous-traitant de lui communiquer toutes informations dont il a besoin pour l'accomplissement de ses missions ;
    - Mener des enquêtes sous la forme d'audits sur la protection des données ;
    - Procéder à un examen des certifications ;
    - Notifier au responsable du traitement ou au sous-traitant une violation alléguée du présent règlement ;
    - 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 ;
    - 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.
- Pouvoir d'adopter toutes les mesures correctrices :
    - Avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer le RGPD ;
    - Rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation du RGPD ;
    - Ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits ;
    - Ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du RGPD ;
    - Ordonner au responsable du traitement de communiquer à la personne concernée une violation ;
    - Imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ;

- Ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement ;

- 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 ;

- Imposer une amende administrative en application de l'article 83, en complément ou à la place des mesures visées au présent paragraphe, en fonction des caractéristiques propres à chaque cas ;

- Ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.

- Pouvoir d'autorisation et consultatif :

  - Conseiller le responsable du traitement conformément à la procédure de consultation préalable ;

  - Emettre, de sa propre initiative ou sur demande, des avis à l'attention du parlement national, du gouvernement de l'État, d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel ;

  - Autoriser le traitement visé à l'article 36 paragraphe 5 ;

  - Rendre des avis sur les projets de code de conduite et les approuver ;

  - Agréer des organismes de certification ;

  - Délivrer des certifications et approuver des critères de certification ;

  - Adopter les clauses types de protection des données ;

  - Autoriser les clauses contractuelles ;

  - Autoriser les arrangements administratifs ;

  - Approuver les règles d'entreprise contraignantes en application de l'article 47.

L'autorité de contrôle peut porter toute violation du RGPD à l'attention des autorités judiciaires : ester en justice.

5) Rapport annuel

L'autorité de contrôle doit établir un rapport annuel sur ses activités, qui peut comprendre une liste des types de violations notifiées et des types de mesures prises.

Ces rapports sont transmis au parlement national, au gouvernement et à d'autres autorités désignées par le droit interne. Ils sont mis à la disposition du public, de la Commission et du Comité.

7. Les sanctions et voies de recours

a) Les sanctions

Au-delà d'un principe de responsabilité qui peut être solidaire, le RGPD prévoit deux types de sanctions. Les amendes administratives et les sanctions à proprement parler.

1) Responsbailité

Le RGPD prévoit que toute personne ayant subi un préjudice (matériel ou moral) du fait d'une violation d'une des dispositions prévues dans le texte, peut ester en justice pour obtenir réparation auprès du responsable du traitement, du sous-traitant ou des deux à la fois (article 82 - principe de co-responsabilité).

Afin de garantir une réparation effective à la personne concernée par la violation de ses droits, le règlement prévoit que le ou les responsables du traitement, ou son ou ses sous-traitants ou les deux en même temps, sont solidairement responsables du dommage. Dans le cas d'une responsabilité solidaire, le responsable du traitement ou le sous-traitant ayant réparé le dommage en totalité peut réclamer 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.

La seule exonération de responsabilité évoquée par le Règlement, consiste pour le responsable du traitement ou son sous-traitant à démontrer que le dommage subi ne lui est pas imputable ; la charge de la preuve lui appartenant.

2) Amendes administratives

Les amendes visent à sanctionner les atteintes aux dispositions des articles 5 (principes relatifs au traitement des données à caractère personnel - licéité, loyauté, transparence), 6 (conditions de licéité du traitement) et 7 (conditions applicables au consentement) du Règlement.

→ *NB : l'article 82 du Règlement parle des atteintes aux articles 4, 5 et 6.*

Les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j) du Règlement (voir fiche relative aux pouvoirs de l'autorité de contrôle). Elles doivent être effectives, proportionnées et dissuasives.

Le Règlement préconise l'analyse d'un certain nombre d'éléments pour décider s'il y a lieu d'imposer une amende administrative, et pour décider de son montant.

Il s’agit des éléments suivants :

- la nature, la gravité et la 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 fait que la violation ait été commise délibérément ou par négligence ;
- toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;

- le 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 et 32 du Règlement (protection des données dès la conception ou par défaut et sécurité du traitement) ;

- toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;

- le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;

- les catégories de données à caractère personnel concernées par la violation ;

- 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 ;

- lorsque des mesures visées à l'article 58, paragraphe 2 (mesures correctrices de l’autorité de contrôle), ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ;

- 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 ;

- 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.

Le montant des amendes varie en fonction des violations ; **le montant le plus élevé étant retenu :**

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.	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.
a. violations des obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 8, 11, 25 à 39, 42 et 43 du règlement ;	a. violations des principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 5, 6, 7 et 9 ;
b. violations des obligations incombant à l'organisme de certification en vertu des articles 42 et 43	b. violations des droits dont bénéficient les personnes concernées en vertu des articles 12 à 22 ;
c. violations des obligations incombant à l'organisme chargé de suivi des codes de conduite en vertu de l'article 41, paragraphe 4.	c. violations des dispositions concernant 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 ;
	d. violations de toutes les obligations découlant du droit des États membres adoptées en vertu du chapitre IX ;
	e. 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, paragraphe 2 (dans ce cas le montant le plus élevé est retenu), ou le fait de ne pas accorder l'accès prévu, en violation de l'article 58, paragraphe 1.

ATTENTION : Si un responsable de traitement ou un sous-traitant viole délibérément ou par négligence plusieurs dispositions du Règlement, 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.

Sans préjudice des pouvoirs dont les autorités de contrôle disposent en matière d'adoption de mesures correctrices en vertu de l'article 58, paragraphe 2, 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. Par ailleurs, la mise en place des amendes administratives est soumise à des garanties procédurales appropriées conformément au droit de l'Union 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 qui lui sont propres, l'article 83 du Règlement (sur les amendes administratives) pourra être appliqué de telle sorte que l'amende sera déterminée par l'autorité de contrôle compétente (CNIL) et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soient effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle.

Les États membres concernés doivent notifier à la Commission les dispositions légales qu'ils adoptent en vertu de l'article 83 du Règlement, au plus tard le 25 mai 2018 et, sans tarder, toute disposition légale modificative ultérieure.

3. Sanctions

Outre les amendes administratives prévues dans le Règlement, il est donné aux États membres la possibilité de déterminer un régime de sanctions autres que les amendes, applicable en cas de violations du Règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83.

Les Etats membres prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions doivent être effectives, proportionnées et dissuasives.

Chaque État membre doit notifier à la Commission les dispositions légales qu'il entend adopter, s'il instaure ces sanctions, au plus tard le 25 mai 2018 et, sans tarder pour toute modification ultérieure les concernant.

b) Les voies de recours

Le RGPD prévoit un véritable droit au recours, quel que soit l'origine du dommage subi par une personne concernée par un traitement de données. Les recours sont intentés par ladite personne ou bien un organisme spécifique dont c'est l'objet. Le Règlement prévoit enfin une certaine collaboration entre les différentes juridictions pouvant être saisies.

1. Droit au recours

Outre les droits reconnus par le Règlement et énumérés plus haut, dans la partie « Droits de la personne concernée », le RGPD reconnait un véritable droit au recours au profit des personnes lésées, issu d'une violation des dispositions dudit règlement.

Les articles 77, 78 et 79 du Règlement introduisent respectivement :

- Un droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- Un droit au recours juridictionnel effectif contre une autorité de contrôle ;
- Un droit à un recours juridictionnel effectif contre un responsable de traitement ou un sous-traitant.

2. Devant l'autorité de contrôle

Toute personne concernée par une violation des dispositions du Règlement a le droit d'introduire, sans préjudice d'autres possibilités de recours, une réclamation auprès de l'autorité de contrôle.

L'autorité de contrôle peut être celle du pays de résidence habituelle du plaignant, ou bien celle de son lieu de travail ou encore celle du pays où a eu lieu la violation.

L'autorité de contrôle saisie a un devoir d'information à l'égard du plaignant et l'informe de l'état d'avancement et de l'issue de sa réclamation, ainsi que de la possibilité de formuler concomitamment un recours juridictionnel.

3. Contre l'autorité de contrôle

Un recours juridictionnel contre une autorité de contrôle est possible devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie.

Le Règlement consacre en effet un droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne, et ce notamment quand ladite autorité de contrôle 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.

4. Contre un responsable de traitement ou un sous-traitant

Toute personne considérant que les droits que lui confère le Règlement ont été violés du fait d'un traitement de ses données à caractère personnel a le droit d'introduire un recours juridictionnel effectif.

Toute action est intentée devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement. 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.

5. Représentation des personnes concernées par un litige

L'article 80 du RGPD prévoit que 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, pour la représenter.

Les objectifs statutaires de cet organisme sont d'intérêt public et il doit être 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, exerce les droits visés aux articles 77, 78 et 79 et exerce le droit d'obtenir réparation lorsque le droit d'un État membre le prévoit, en leur nom.

Les États membres peuvent prévoir que cet organisme, organisation ou association, 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, et d'exercer les droits visés aux articles 78 et 79 s'il considère que les droits d'une personne concernée prévus dans le Règlement ont été violés du fait du traitement.

6. Principe de la suspension d'une action

Afin d'éviter les dédoublements de procédures concernant une même affaire, le Règlement prévoit dans son article 81 que toutes les juridictions d'un État membre informées 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, doivent contacter cette juridiction dans l'autre État membre pour confirmer l'existence d'une telle action.

De fait, toute juridiction compétente autre que la juridiction saisie en premier lieu pourra suspendre son action.

Enfin, lorsqu'une action sera pendante devant des juridictions du premier degré, toute juridiction autre que la juridiction saisie en premier lieu pourra 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.

8. Les prestataires auxquels faire appel pour se mettre en conformité

Afin de mettre en œuvre le RGPD, il est possible, voire souhaitable, de prendre conseil auprès d'un cabinet spécialisé en protection de données personnelles.

Regroupés au sein d'une association, les cabinets conseils apportent non seulement leur expertise dans l'application du Règlement, mais aussi un œil extérieur sur l'organisation et l'utilisation des données personnelles dans l'entreprise ou la collectivité.

Cette association très éclectique regroupe également des correspondants désignés par leur organisme ou leur collectivité auprès de la CNIL, les futurs DPO, des cabinets d'avocats, des prestataires informatiques et des experts en sécurité.

Cet accompagnement permettra de répondre à plusieurs besoins dont notamment :

- Le recensement et cartographie des traitements réalisés dans l'entreprise et recommandations à mettre en place ;
- L'audit de la sécurité et de la confidentialité des données ;
- L'assistance à la tenue du registre des traitements et de tableaux de bord de suivi de la conformité ;
- Les définitions des moyens d'information et des codes de conduite précisant les procédures de respect des droits de la personne ;
- L'assistance à la mise en place d'une démarche d'amélioration continue ISO 27001 (norme internationale des systèmes de gestion de la sécurité de l'information)
- La formation ou externalisation du CIL / DPO ;
- La sensibilisation des personnels sur la protection des données à caractère personnel…

L'entreprise ou la collectivité qui souhaite se faire accompagner dans la mise en œuvre des nombreuses obligations issues du RGPD peut donc choisir, parmi un panel d'acteurs, l'entreprise ou le cabinet qui lui correspond le mieux.

Une analyse des compétences et de la pérennité du prestataire est indispensable. En effet, une trentaine d'acteurs se sont déjà positionnés sur le marché actuellement et tous ne présentent pas les mêmes critères en terme de taille ou de chiffre d'affaires. Beaucoup sont notamment de création très récente et peuvent présenter des risques de défaillance. Il est aisé d'imaginer les conséquences désastreuses pour l'entreprise ou la collectivité, si le prestataire venait à disparaître durant le processus d'audit ou de mise en place des codes de conduite.

9. L'impact du RGPD sur les personnes publiques

Selon les statistiques de la CNIL, 2/3 des régions, la moitié des départements, 2/3 des métropoles, 1/3 des communautés urbaines, 1/10e des communautés d'agglomération, et seulement 2% des communes ont désigné un correspondant informatique et libertés (CIL).

Selon une étude menée par la Gazette des communes, seules 10% des communes estimaient en juillet 2017 qu'elles seraient prêtes pour l'application du RGPD au 25 mai 2018 ; date à laquelle il devient directement applicable dans les Etats membres.

a) Les enjeux

Les personnes publiques et notamment les collectivités territoriales sont au cœur d'une évolution globale qui intègre plusieurs objectifs de transparence, de disponibilité et d'accès des documents administratifs, et de développement du numérique. Une première étape avait été instaurée par la loi pour une République numérique en octobre 2016, codifiée notamment dans le code des relations entre le public et l'administration. Le Règlement européen constitue une suite dans cette évolution.

Au même titre que les autres acteurs responsables de traitement des données, les personnes publiques seront soumises aux obligations découlant du Règlement, et potentiellement au risque de sanctions qu'il énumère également.

b) Les personnes publiques actrices de la protection des données

Les personnes publiques, à l'instar des acteurs privés développent toujours plus l'utilisation des traitements de données, et seront soumises aux obligations et procédures recensées dans le Règlement européen.

Les collectivités territoriales et globalement toutes les personnes morales de droit public devront s'imposer ainsi une logique de responsabilisation et mettre en conformité leurs pratiques.

Elles seront dès lors également assujetties aux principes de protection des données dès la conception du traitement (Privacy by design) et par défaut (Privacy by default).

La CNIL enjoint dès lors les collectivités territoriales à « *tenir un registre de leurs activités de traitement, à encadrer les opérations sous-traitées dans les contrats de prestation de services, à formaliser des politiques de confidentialité des données, des procédures relatives à la gestion des demandes d'exercice des droits, à adhérer à des codes de conduite ou encore à certifier des traitements (…) pour les traitements à risques, elles devront effectuer des analyses d'impact sur la vie privée et notifier à la CNIL, voire aux personnes concernées, les violations de données personnelles* ».

c) Le délégué à la protection des données (DPD/DPO)

Dès le 25 mai 2018, la désignation d'un délégué à la protection des données, successeur du correspondant informatique et libertés (CIL), dont la désignation est aujourd'hui facultative, sera obligatoire pour les organismes et autorités publiques, et donc pour les collectivités.

Le constat est parlant, les collectivités territoriales n'ont que rarement mis en place les CIL. Le changement imposé par le RGPD est d'imposer le délégué à la protection des données à toutes les personnes publiques.

La CNIL propose une solution et indique expressément aux collectivités de mutualiser leur DPO *via* des structures de mutualisation informatique, spécialisées dans le développement de l'e-administration sur leur territoire.

10. Les spécificités applicables aux Ressources Humaines

L'employeur est tenu de respecter les obligations développées dans les fiches précédentes. Le RGPD prévoit toutefois quelques spécificités en matière de droit social.

Ainsi, les Etats membres peuvent prévoir des règles légales ou conventionnelles pour les traitements de données personnelles de salariés notamment concernant le recrutement, l'exécution du contrat de travail, l'organisation du travail, l'égalité et la diversité, la santé et la sécurité, la protection des biens de l'entreprise ou de ses clients, l'exercice ou la jouissance de droits et la rupture du contrat de travail (article 88 du RGPD). *« Ces règles comprennent des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière à la transparence du traitement, au transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe et aux systèmes de contrôle sur le lieu de travail ».*

En principe, les traitements ne doivent pas porter sur les données suivantes :

- Race ;
- Ethnie ;
- Opinions politiques ;
- Convictions religieuses ou philosophiques ;
- L'appartenance syndicale ;
- Santé ;
- Vie sexuelle ;
- Orientation sexuelle ;
- Données génétiques ;
- Données biométriques.

Toutefois, il peut être possible de déroger à ce principe en droit social afin de permettre aux employeurs de respecter leurs obligations légales en matière de droit du travail, de Sécurité sociale et de protection sociale et à condition que le traitement soit encadré par des dispositions légales ou conventionnelles (article 9 du RGPD).

Annexes

Thème des articles	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.	Règlement 2016-679 du parlement européen et du conseil.
Principes généraux et définitions		
Champ d'application du texte	2, 4, 5	2, 3
Définitions	2,3	4
Conditions relatives au traitement (manipulation) des données	6	5
Conditions relatives aux traitements/fichiers	7	6
Consentement	x	7, 8
Données sensibles	8	9
Personnes compétentes pour les traitements de données relatives aux infractions, condamnations et mesures de sûreté	9	10
Traitement ne nécessitant pas d'identification	x	11
Décision de justice et/ou individuelle fondée sur les données personnelles	10	22
CNIL (loi de 78) et Autorité indépendante (Règlement)		
Entité	x	51
Indépendance	x	52
Missions	11	55, 56, 57
Finances	12	54
Composition	13	53, 54
Incompatibilité	14	54
Formation plénière	15	54
Bureau	16	54
Pouvoirs et sanctions	17	58
Commissaire du gouv.	18	54
Commission	19	54
Secret professionnel	20	54
Souveraineté	21	52
Rapport d'activité	x	59
Réclamation devant l'autorité de contrôle		77
Recours à l'encontre de l'autorité de contrôle		78
Formalités relatives à la mise en œuvre des traitements		
Cas de déclarations et exonérations de	22	

formalité		
Formalisme de la déclaration	23	
Principe de la NS et de la dispense	24	
Autorisation (principe et cas)	25	
Autorisation des traitements de l'Etat	26, 27, 28	
Contenu de l'autorisation	29	
Contenu des déclarations, des demandes d'autorisations et d'avis	30	
Liste des traitements automatisés	31	
Amendes et sanctions		83, 84
Droits des personnes concernées		
Droit à l'information	32	12, 13,14
Cas des certificats de signatures électroniques	33	
Droit d'accès	39, 43	15
Droit de rectification	40, 40-1	16, 19
Droit à l'effacement (oubli)	40, 40-1	17, 19
Droit à la limitation du traitement	x	18, 19
Droit à la portabilité du traitement	x	20
Droit d'opposition	38	21
Limitations possibles des droits (conditions)	41, 42	23
Exercice des droits par voie électronique	43 bis	
Droit au recours devant l'autorité de contrôle		79
Représentation des plaignants et action collective		80
Droit à réparation		82
Obligations (autres que les droits des personnes concernées) du responsable du traitement		
Responsabilité du responsable du traitement		24 et 26 (responsabilité conjointe), 82
Devoir de préservation des données	34	25, 32
Mécanisme en cas de violation des données	34 bis	33, 34
Sous-traitance	35	28, 29, 30, 31
Conservation des données limitée	36	
Registre des activités de traitement	x	30
Coopération avec l'autorité de contrôle		31
Analyse d'impact sur la vie privée en cas de traitement sensible	x	35, 36
Correspondant informatique et libertés (CIL) et Délégué à la protection des données (DPD)		
CIL	22	x
Désignation du DPD	x	37

Fonction du DPD	x	38
Missions du DPD	x	39
Codes de conduite et certification		
Codes de conduite	x	40, 41
Certification (labélisation) des traitements	x	42, 43
Transferts de données vers pays tiers ou OI		
Conditions relative au responsable du traitement	x	44
Conditions relatives à l'entité d'accueil (pays ou OI) des données	68	45 (décision d'adéquation) 46 (garantie appropriée)
Règles d'entreprises contraignantes	69	46, 47
Transfert demandé par juridiction et administration de pays tiers	x	48
Dérogations	69	49
Interdictions	70	
Coopération internationale	x	50
Coopération		
Coopération entre autorités de contrôle	x	60
Assistance mutuelle	x	61
Opération conjointe	x	62
Suspension d'une action devant une autorité de contrôle (même litige devant juridiction de plusieurs états membres)	x	81
Cohérence dans l'application du Règlement		
Principe de la cohérence de l'application du règlement	x	63
Avis du Comité (CEPD)	x	64
Règlement des litiges	x	65
Procédure d'urgence	x	66
Echange d'information	x	67
Comité européen de la protection des données		
CEPD	x	68, 69
Missions	x	70
Rapport	x	71
Procédure	x	72, 76
Président	x	73, 74
Secrétariat	x	75
Préconisations aux Etats membres		
Combinaison protection des données et	x	85

liberté d'expression/presse		
Liaison avec CADA	15 bis	86
Numéro d'identification national		87
Combinaison protection des données et droit du travail		88
Cas des traitements d'archives d'intérêt public/scientifique/historique/statistique		89
Obligation de secret		90
Relation avec le culte		91

Comment SVP peut vous être utile ?

Née en 1935, SVP fournit de l'information opérationnelle aux décideurs, en entreprise et collectivité, pour les aider au quotidien dans leur pratique professionnelle. Elle leur apporte pour cela les réponses immédiates dont ils ont besoin pour gérer et développer leurs activités.

La société accompagne à ce jour 7 000 clients et 30 000 décideurs grâce à 200 experts organisés par domaine de compétences : ressources humaines, fiscalité, vie des affaires, communication/marketing, finance, sourcing...

Grâce à leurs compétences multiples et aux outils documentaires sans équivalent mis à leur disposition, ces experts répondent ainsi en toute confidentialité – et principalement par téléphone - à près de 2 000 questions posées quotidiennement.

Offre spéciale livre blanc :

Nous vous remercions d'avoir téléchargé notre livre blanc sur le Règlement sur la Protection des données personnelles.

Les experts vous proposent maintenant de tester gratuitement le service SVP en posant une première question.

Posez votre question : nos experts vous répondent !

http://offre.svp.com/campagne/question/qi-lb-rgpd/

