MANDIL AVOCATS

La protection des données personnelles en quelques fiches

Présentation - Février 2020

Entrepreneurs, salariés, consommateurs et/ou utilisateurs de services numériques, nous sommes tous concernés par la protection des données à caractère personnel. Nous disposons à ce titre de droits et devons respecter certaines obligations.

L'objet de ces fiches est de présenter de manière synthétique les règles applicables en cas de traitement de telles données.

A savoir

Le contexte de la protection des données personnelles

Les données personnelles sont au cœur de la révolution numérique. L'exploitation commerciale de ces données peut avoir des conséquences sur la vie privée des individus.
Les législations françaises et européennes reposent sur cette recherche d'un compromis entre protection de la vie privée, innovation technologique et croissance économique.

Fiche 01 — Périmètre de la protection des données

Fiche 02 — Les grands principes du RGPD

Fiche 03 — Sur quel fondement traiter des données personnelles ?

Fiche 04 — Privacy by design & privacy by default

Fiche 05 — Analyse d'impact sur la vie privée

Fiche 06 — Le Délégué à la protection des données

Fiche 07 — RGPD : comment protéger les droits des individus ?

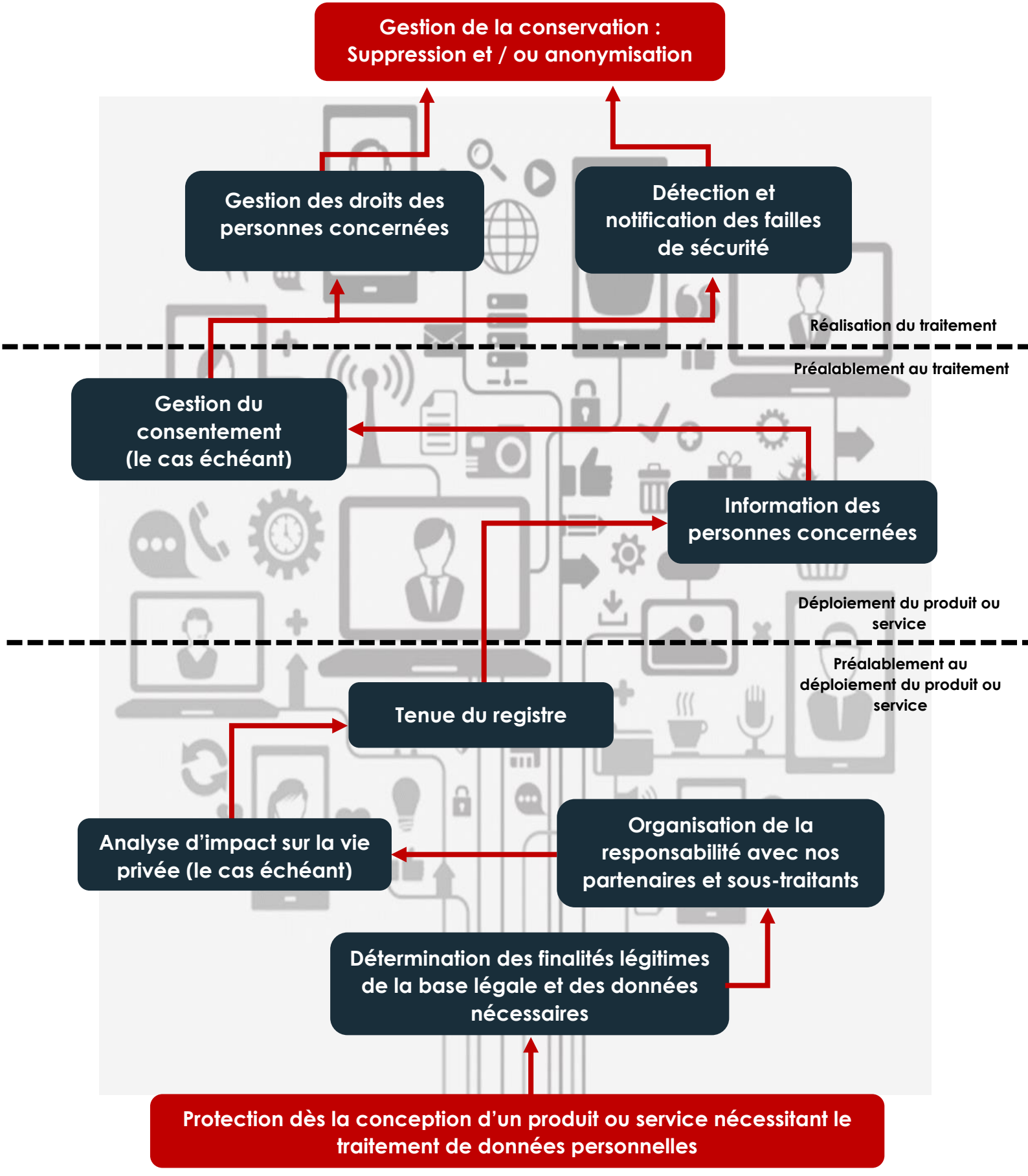
Fiche 08 — Violations de données personnelles

Fiche 09 — Conservation, anonymisation et suppression

Fiche 10 — Transferts de données hors de l'EEE

Fiche 11 — Sanctions en cas de manquement au RGPD

Le cycle d'un traitement de données personnelles !



MANDIL AVOCATS

MANDIL AVOCATS

Le périmètre de la protection des données personnelles

Fiche n°01 - Janvier 2020

Parfois qualifiées de « pétrole du XXIe siècle », les données à caractère personnel (« données personnelles ») sont fondamentales pour l'économie numérique. Elles permettent notamment de produire un profil précis des individus.

Pour limiter les risques d'atteintes à la vie privée que causerait leur exploitation commerciale incontrôlée, la France et l'Union européenne ont instauré un cadre légal protégeant les données personnelles sans pour autant freiner l'innovation.

A savoir

La protection des données, un droit fondamental !

La protection des données personnelles est un droit fondamental notamment garanti dans l'UE par l'article 286 du **traité instituant la Communauté européenne** et par l'article 8 de la **Charte des droits fondamentaux de l'UE** ainsi que dans l'Europe par l'article 8 de la Convention européenne des droits de l'homme (**CEDH**) proclamant le droit de toute personne au respect « *de sa vie privée et familiale, de son domicile et de sa correspondance* ».

I. Quels sont les textes protégeant les données personnelles ?

1. Un cadre européen harmonisé…

Le règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données personnelles (RGPD) abroge l'ancienne directive 95/46/CE du 24 octobre 1995 et :

- Harmonise la règlementation européenne
- Renforce le champ d'application territorial (extraterritorialité)
- Prévoit de nouveaux droits
- Supprime la plupart des formalités préalables
- Renforce fortement les sanctions pécuniaires

Le RGPD est complété par la Directive (UE) 2016/680 adoptée le même jour qui concerne les **traitements réalisés par les autorités en matière pénale** (prévention, enquête, sanction…).

2. …précisé par la loi française

La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a été modifiée, en particulier, par les lois **n° 2016-1321 du 7 octobre 2016** et **n° 2018-493 du 20 juin 2018** et par le décret d'application **n° 2019-536 du 29 mai 2019**. Elle complète et précise la règlementation européenne :

- Instaure un droit à la mort numérique
- Renforce les pouvoirs de la CNIL
- Conserve des formalités préalables en matière de santé
- Transpose la Directive 2016/680 « police-justice »
- Régit les traitements concernant la défense nationale ou la sûreté de l'Etat

II. Qu'est-ce qu'une donnée à caractère personnel ?

Une donnée à caractère personnel est une information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement. Les données dites « sensibles » ou relatives aux infractions sont soumises à un régime spécifique.

Identité : nom et prénom

Numéros d'identification : Plaque d'immatriculation, numéro de CNI ou de passeport…

Vie privée : date de naissance, statut marital, nombre d'enfants, adresse…

Données de communication : identifiant/mot de passe, cookies, adresse IP…

Données relatives à des condamnations ou infractions pénales

Habitudes de vie : activités culturelles ou sportives, habitudes d'achat et de consommation, vie sociale…

Vie professionnelle : poste, coordonnées professionnelles, évaluation…

Image/son : photo, vidéo, enregistrement vocal…

Données de localisation : GPS, données GSM…

Informations financières : numéro de carte bancaire et de compte bancaire, revenus…

Données sensibles : numéro de sécurité sociale, origine ethnique, santé, biométrie, opinions politiques et religieuses, appartenance syndicale…

Cf. Fiche n°09

Lorsque ces données sont anonymisées, c'est-à-dire qu'elles ne peuvent pas être reliées directement ou indirectement à un individu, elles ne sont plus considérées comme des données personnelles et ne relèvent plus de la règlementation applicable.

III. Qu'est ce qu'un traitement de données personnelles ?

Un traitement de données personnelles consiste en **toute opération effectuée sur des données personnelles**. Un traitement peut ainsi être composé de plusieurs opérations liées : collecte, diffusion, conservation, archivage et suppression de données par exemple.

Le traitement peut être automatisé (à l'aide d'un ordinateur) ou non. Sont exclues les traitements réalisés à titre exclusivement **domestique ou personnel** (liste d'invités pour un mariage par exemple).

IV. Quels sont les acteurs concernés et visés par le RGPD ?

Autorités compétentes

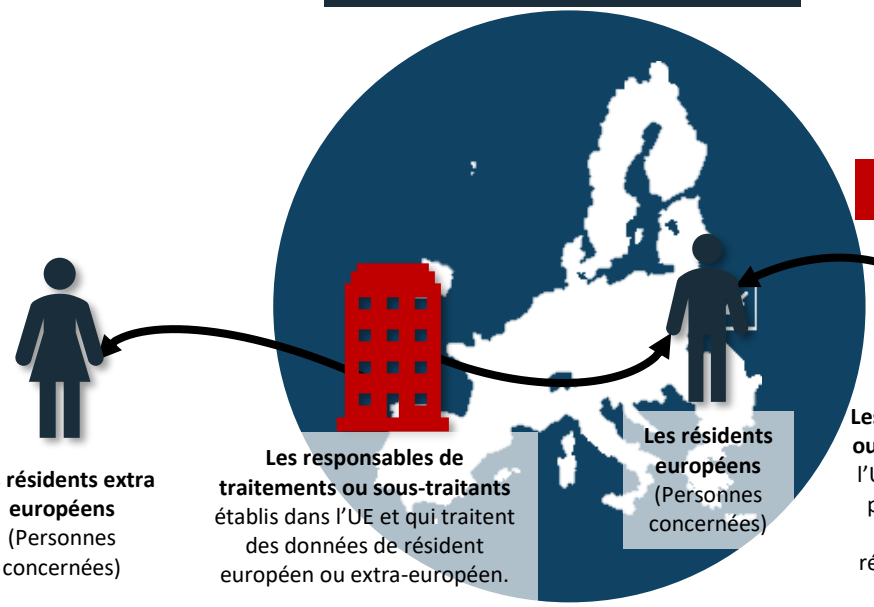
CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

La **Commission nationale de l'informatique et des libertés est** l'autorité administrative indépendante compétente pour contrôler la conformité des traitements de données personnelles.

edpb European Data Protection Board

Le **Comité européen de protection des données** (**EDPB** en anglais) est un organe indépendant de coopération entre les autorités européennes chargé d'harmoniser l'application du RGPD.

Champ d'application territorial



Les résidents extra européens (Personnes concernées)

Les responsables de traitements ou sous-traitants établis dans l'UE et qui traitent des données de résident européen ou extra-européen.

Les résidents européens (Personnes concernées)

Les responsables de traitements ou sous-traitants établis hors de l'UE et qui traitent des données personnelles pour fournir des biens et des services aux résidents européens, y compris par Internet.

Le responsable du traitement est l'entité (personne physique ou morale, autorité, service…) qui **détermine les finalités et / ou les moyens essentiels** (durée de conservation, mesure de sécurité, destinataires…) d'un traitement, **seule ou conjointement avec un autre.**

Cf. Fiche n°12

Le sous-traitant est l'entité qui traite des données personnelles pour le compte du responsable du traitement.

Le sous-traitant ultérieur est le sous-traitant d'un sous-traitant. Il agit sous la responsabilité de ce dernier.

Le fait de traiter directement soi-même ou non les données personnelles n'est pas un critère pour déterminer si l'on est responsable du traitement.

Un tiers est une entité autre que la personne concernée, le responsable du traitement ou le sous-traitant.

Par exemple, un autre **responsable du traitement distinct**.

Un destinataire est une entité qui reçoit des données personnelles, qu'il s'agisse ou non d'un tiers.
Les autorités publiques légitimes à se faire communiquer des données ne sont pas des destinataires.

Le **Délégué à la protection des données** (**DPO** en anglais) est la personne chargée de la protection des données au sein d'une organisation.

Cf. Fiche n°06

MANDIL AVOCATS

MANDIL AVOCATS

Comprendre le RGPD en 10 grands principes

Fiche n°02 - Janvier 2020

Le RGPD prévoit 10 grands principes permettant de s'assurer que les traitements de données personnelles réalisés sont nécessaires, proportionnés et réalisés de manière sécurisée. Contrairement à l'ancien régime de formalités préalables auprès de la CNIL, il repose sur une logique de responsabilisation et de transparence des responsables de traitements et des sous-traitants qui doivent documenter leur conformité tout au long du traitement.

I. Licéité du traitement

Le traitement doit se fonder sur **une des 6 bases légales** suivantes : Cf. Fiche n°03

Consentement de la personne concernée

Exécution d'un contrat auquel la personne concernée est partie

Respect d'une obligation légale

Exécution d'une mission d'intérêt public

Sauvegarde des intérêts vitaux

Intérêt légitime du responsable du traitement

II. Limitation des finalités

Les données doivent être collectées pour des finalités :

- **Déterminées** : précisément identifiées en amont de la collecte ;
- **Explicites** : clairement exprimées de façon intelligible dès la collecte des données ;
- **Légitimes** : fondées sur l'une des 6 bases légales et conformes à la loi.

Elles ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités (**le détournement de finalité est une infraction pénale**).

SAUF si le traitement ultérieur :

- A obtenu le consentement de la personne concernée ;
- Repose sur une finalité « compatible » avec la finalité initiale ;
- Est réalisé à des fins archivistiques dans l'intérêt public, de recherche scientifique ou historique, ou statistiques.

III. Minimisation

Seules doivent être traitées les données personnelles **adéquates, pertinentes et limitées à ce qui est nécessaire** au regard des finalités pour lesquelles elles sont traitées.

Exemple : un site internet non marchand n'a pas a priori pas besoin de collecter le numéro de carte bancaire d'un internaute.

IV. Exactitude

Le responsable du traitement doit veiller à ce que les données soient **exactes et, si nécessaire, tenues à jour, effacées ou rectifiées** sans tarder.

V. Limitation de la conservation

Les données doivent être **conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités** pour lesquelles elles sont traitées.

A terme, elles doivent être **supprimées ou anonymisées**.

Cf. Fiche n°09

Comprendre le RGPD en 10 grands principes

VI. Intégrité & confidentialité

Des **mesures de sécurité techniques, physiques et organisationnelles** appropriées doivent être prise pour limiter les risques d'accès, de modification et de suppression non autorisés des données.

Recours à des méthodes de chiffrement ou de pseudonymisation

Limitation des accès aux seuls destinataires (internes et externes) **nécessaires et légitimes**

Principe d'interdiction des transferts de données hors de l'EEE

Cf. Fiche n°10

VII. Transparence

Le responsable du traitement doit préalablement informer la personne concernée par le traitement des :

Mentions légales obligatoires (identité du responsable du traitement, finalité du traitement, durée de conservation des données…)

+

Droits de la personne concernée et de sa possibilité d'adresser une réclamation à la CNIL

Cf. Fiche n°07

VIII. Loyauté et droits des personnes concernées

La personne concernée bénéficie de nombreux droits garantis par le **Chapitre III du RGPD et la Loi de 1978** : Cf. Fiche n°07

Accès | **Portabilité** | **Rectification** | **Effacement / oubli** | **Opposition** | **Limitation** | **Mort numérique** (Loi de 78)

IX. Responsabilité (accountability)

Le responsable du traitement doit **documenter le traitement pour être en mesure de démontrer** sa conformité au RGPD.

Tenue du registre des traitements

Cf. Fiche n°05

Désignation d'un délégué à la protection des données

Cf. Fiche n°06

Accountability

Réalisation des analyses d'impact sur la vie privée

Obtention de certifications et conformité à des codes de conduite

Détection et notification des violations de données

Cf. Fiche n°08

X. Protection dès la conception & par défaut

La conformité aux dispositions du RGPD doit être anticipée par des mesures appropriées **dès la conception d'un produit ou d'un service**

+

Par défaut, des mesures doivent être prises pour limiter le traitement à ce qui est strictement nécessaire

Cf. Fiche n°04

MANDIL AVOCATS

MANDIL AVOCATS

Sur quel fondement traiter des données personnelles ?

Fiche n°03 - Février 2020

L'article 5.1 a) du RGPD dispose que les données personnelles doivent être traitées de manière licite. Pour ce faire, tout traitement de données doit préalablement se fonder sur l'une des « bases légales » prévues par l'article 6.1 du RGPD. Le RGPD ne crée pas de hiérarchie entre les différentes bases légales. Par exemple, le consentement ne prévaut pas sur les autres.

Lorsqu'un même traitement de données poursuit plusieurs finalités, une base légale doit être définie pour chacune d'entre elles. En revanche, il n'est pas possible de « cumuler » des bases légales pour une même finalité : il faut en choisir une seule.

Attention : les droits des personnes concernées dépendent de la base choisie ! Cf. Fiche n°07

A savoir — **La détermination de la finalité du traitement**

Le traitement de données personnelles doit s'inscrire dans un but précis. Cette finalité doit être déterminée, légitime et explicite. Sauf exception **(Cf. Fiche n°01)**, il n'est pas possible d'utiliser les données personnelles pour une autre finalité que celle qui a été préalablement définie. **Attention : le détournement de finalité est une infraction pénale !**

I. Le consentement

Le consentement de la personne concernée est l'une des 6 bases légales prévues par le RGPD : il n'est donc pas systématique. **Il est en revanche parfois prévu par la loi** dans certains cas : cookies, prospection commerciale, levée du secret bancaire…).

Pour être valablement recueilli, le consentement doit être :

Préalable : il n'est pas possible de recueillir le consentement a posteriori.

Libre : il ne doit pas être contraint ni influencé :
- **Pas de déséquilibre des rapports de force** : autorité publique /administré ou employeur/employé…
- **Pas de préjudice ou d'impact sur l'exécution d'un contrat** en cas de refus de consentir.

Spécifique : un consentement doit correspondre à un seul traitement, pour une finalité déterminée. En cas de finalités multiples, il doit pouvoir être possible de **consentir indépendamment pour chacune d'elles**.

Eclairé : la personne doit être informée de l'étendue du traitement (identité du responsable du traitement, finalité, données, retrait possible du consentement…).

Univoque : il doit consister en une déclaration de la part de la personne concernée ou un acte positif clair. **L'utilisation d'une case pré-cochée est prohibée tout comme l'acceptation globale d'un contrat / CGU….**

Révocable : il doit pouvoir être **retiré à tout moment**.

Documenté : il revient au responsable du traitement de prouver que le consentement a été recueilli.

II. L'exécution d'un contrat

Le traitement peut se fonder sur cette base lorsqu'il est :

- **nécessaire** à l'exécution d'un contrat (y compris la phase précontractuelle) : CGV, contrat de travail…
- auquel la **personne concernée est partie**
- et que ce **contrat respecte les dispositions nationales du droit des contrats**.

Le responsable du traitement doit être capable de démontrer que l'objet même du contrat ne peut être exécuté si le traitement de données n'a pas lieu :

- C'est en principe le cas des traitement suivants : adresse postale à des fins de **livraison**, **informations de la carte bancaire afin de permettre le paiement**…
- Ce n'est en principe pas le cas des traitements suivants : **amélioration du service**, **prévention de la fraude, vidéosurveillance, action en justice, publicité comportementale, lutte contre le blanchiment**…

Mentionner le traitement dans le contrat n'est pas suffisant : le traitement doit réellement correspondre à l'esprit du service visé par le contrat. Dans le cas contraire, une autre base légale doit être déterminée.

Il n'y a pas de droit d'opposition : le traitement prend fin au terme ou à la résiliation du contrat.

Un **consentement explicite** est requis en cas de risque sérieux lié à la protection des données (traitement de données sensibles, transfert hors EEE…). Dans ce cas, le consentement doit être renforcé : consentement en deux étapes ou déclaration signée par exemple.

Sur quel fondement traiter des données personnelles ?

III. Le respect d'une obligation légale

Un traitement peut être justifié lorsqu'il est **nécessaire** au respect d'une obligation légale à laquelle le responsable du traitement est soumis. L'obligation légale doit :

- Être définie par le **droit européen ou national d'un État membre** auquel le responsable est soumis ;
- **Constituer une obligation impérative et contraignante** de traiter des données personnelles, **suffisamment claire et précise** et au moins **définir les finalités** du traitement concerné ;
- **S'imposer au responsable du traitement**, et non aux personnes concernées par le traitement.

Exemple : obligations de l**utte contre le blanchiment** ou de **conservation fiscales, sociales et comptables**.
Contre-exemple : les traitements autorisés mais non obligatoires de **lutte contre la fraude** ou de surveillance.

Les droits d'opposition et à la portabilité ne peuvent pas être exercés par les personnes concernées lorsque le traitement est fondé sur une obligation légale.

V. La sauvegarde des intérêts vitaux

Un traitement peut être mis en œuvre lorsqu'il est **nécessaire** à la **sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne**.

L'intérêt vital concerne :

- des questions de **vie ou de mort** ;
- des menaces qui comportent un **risque de blessure** ou une autre **atteinte à la santé**.

Lorsqu'il est possible et nécessaire de demander un consentement valable, il y a effectivement lieu de se fonder sur le consentement.

Les droits d'opposition et à la portabilité ne peuvent pas être exercés par les personnes concernées lorsque le traitement est fondé sur la sauvegarde des intérêts vitaux.

IV. L'exécution d'une mission d'intérêt public

Cette base légale peut fonder les traitements **nécessaires** à l'**exécution d'une mission d'intérêt public** ou d'une **mission relevant de l'exercice de l'autorité publique** incombant à un organisme. Cette base légale concerne donc les traitements mis en œuvre par :

- Des autorités **publiques** dans le cadre de leurs missions.
- Des organismes **privés**, dès lors qu'ils poursuivent une mission d'intérêt public ou sont dotés de prérogative de puissance publique.

L'intérêt public doit être clairement prévu et défini par le droit européen ou national (règlement, loi, décret…).

VI. La poursuite d'intérêts légitimes

Le responsable du traitement peut se fonder sur cette base légale lorsque le traitement est **nécessaire** aux fins des **intérêts légitimes poursuivis par ce dernier ou par un tiers.**

Il s'agit d'une base légale ne pouvant être utilisée que de manière rigoureuse après un examen attentif :

- **L'intérêt poursuivi doit être « légitime »,** c'est-à-dire licite, clair et précis : lutte contre la fraude, sécurité des biens et des personnes, prospection commerciale (uniquement dans certains cas : BtoB…), gestion administrative interne, …

- **Le traitement ne doit pas créer de déséquilibre au détriment des droits, libertés et intérêts des personnes dont les données sont traitées compte tenu de leurs attentes raisonnables** : l'organisme doit donc opérer une **mise en balance** / pondération entre les droits et ses intérêts en cause.

Le droit à la portabilité ne s'applique pas aux traitements fondés sur l'intérêt légitime.

L'intérêt légitime ne peut pas constituer la base légale d'un traitement mis en œuvre par une autorité publique dans l'exécution de ses missions.

MANDIL AVOCATS

MANDIL AVOCATS

Privacy by Design by Default

Fiche n°04 - Février 2020

L'article 25 du RGPD prévoit deux nouveaux principes en vertu desquels les responsables du traitement, avec l'aide de leurs éventuels sous-traitants, doivent prendre les mesures techniques et organisationnelles appropriées pour que :

- **Dès la conception d'un service ou d'un bien nécessitant un traitement de données personnelles, celui-ci soit conforme aux dispositions du RGPD tout au long de son cycle de vie ;**
- **Par défaut, seules les données personnelles nécessaires soient traitées.**

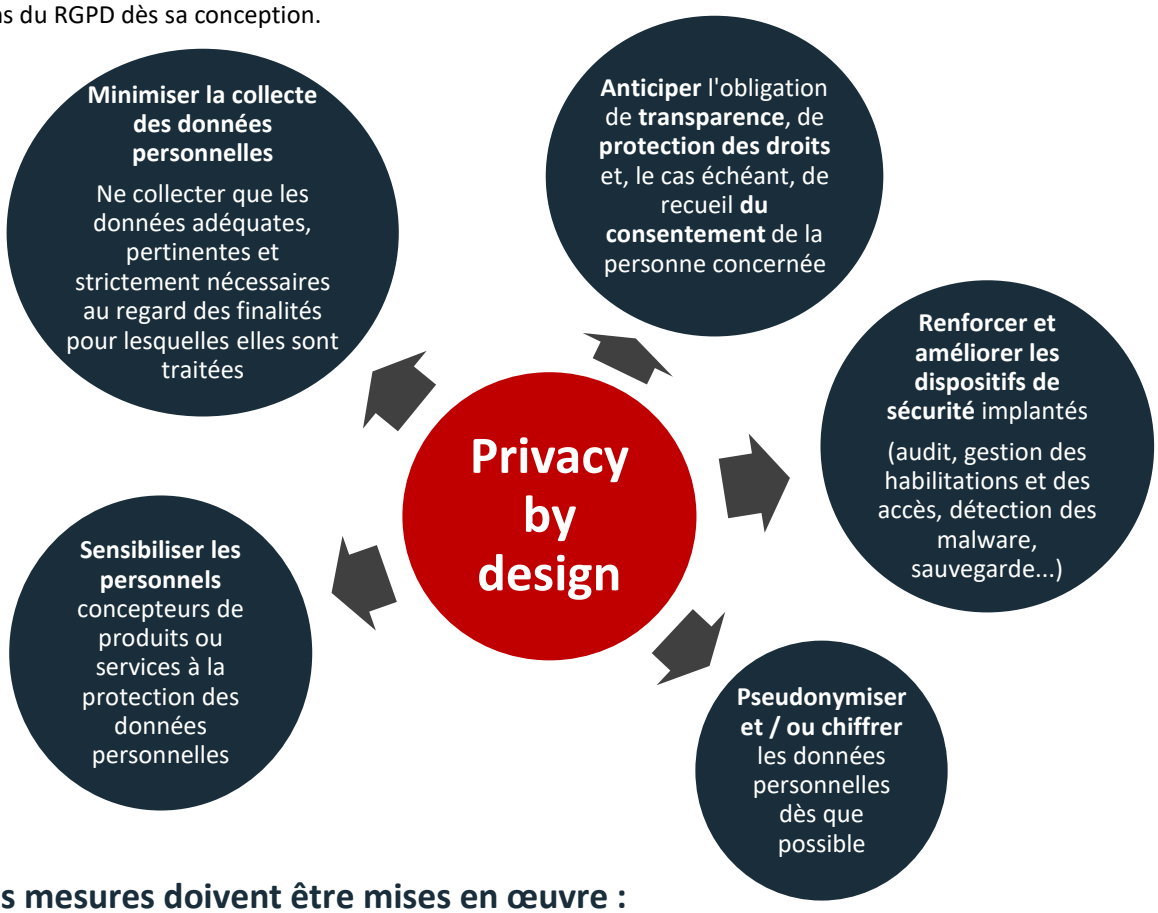
A savoir

Projet de lignes directrices de l'EDPB du 13 novembre 2019

Les autorités européennes (EDPB) ont publié le 13 novembre 2019 leur **projet de lignes directrices** sur les principes de protection des données personnelles dès la conception et par défaut. Celles-ci fournissent des indications sur la manière d'appliquer ces principes en pratique, reconnaissent que les sous-traitants et les fournisseurs de technologies en sont les principaux facilitateurs et incitent l'ensemble des acteurs à en tirer un **avantage concurrentiel**.

I. Le principe de *Privacy by design*

Le responsable du traitement (avec l'aide de ses sous-traitants éventuels) qui conçoit un produit ou un service doit **mettre en œuvre des mesures techniques et organisationnelles** permettant de garantir la conformité de ce service ou produit aux dispositions du RGPD dès sa conception.



Ces mesures doivent être mises en œuvre :

Dès la phase de conception et même de planification d'un bien ou service

Pendant toute la durée du traitement et donc évaluées régulièrement pour rester à jour

Pour déterminer les mesures techniques et organisationnelles appropriées, **les responsables du traitement doivent tenir compte de** :

L'Etat de l'art
Ils doivent se tenir au courant des progrès technologiques et y veiller avec leurs sous-traitants.

Le coût et les ressources nécessaires
Y compris les RH et le coût potentiel des amendes résultant du non-respect du RGPD.

La nature, la portée, le contexte et la finalité du traitement
Notamment pour s'assurer de sa proportionnalité.

Les risques pour les droits et libertés des personnes
Risques d'accès non autorisé, de modification ou de perte des données par exemple.

II. Le principe de *Privacy by Default*

En vertu de ce principe, le responsable du traitement doit adopter des mesures consistant à **limiter, par défaut, le traitement à ce qui est strictement nécessaire**. La limitation peut notamment concerner :

La **quantité de données collectées** (volume, type…)	La **diversité des finalités**	La **durée de conservation** (puis suppression ou anonymisation)	Le **nombre de personnes** habilitées à **accéder** aux données

Exemple d'application du principe de *Privacy by default* : un service en ligne proposant plusieurs niveaux de paramétrage de confidentialité devra être réglé par défaut, lors de l'inscription, sur le niveau le plus protecteur.

A noter

Privacy by design, privacy by default et certification

Les responsables du traitement doivent pouvoir démontrer que les mesures mises en œuvre produisent l'effet souhaité en termes de protection des données : **détermination d'indicateurs clés de performance appropriés (quantitatifs et/ou qualitatifs).**

Les fabricants de produits ou les concepteurs de services peuvent recourir à des mécanismes de certification (labels, marques…) et/ ou adhérer à des codes de conduite qui prévoient la mise en œuvre de mesures techniques et organisationnelles garantissant la protection des données personnelles dès la conception et par défaut.
L'utilisation de ces outils leur permettra de bénéficier d'une présomption de conformité en cas de contrôle par la CNIL.

La certification est une procédure par laquelle un tiers certificateur va donner l'assurance écrite qu'une personne, un produit, un processus ou un service est en conformité avec les exigences d'un référentiel.
La certification est contraignante et doit être renouvelée : elle donne lieu à un contrôle régulier par le tiers certificateur du respect du référentiel via des audits et des examens.
La CNIL peut directement certifier des organismes et agréer des organismes certificateurs ou, selon les cas, choisir de collaborer avec le Comité Français d'Accréditation (COFRAC).

Les codes de conduite sont élaborés par les acteurs professionnels (fédérations, organisations professionnelles) et se composent de bonnes pratiques dans un secteur d'activité donné (durée de conservation, mention d'information, modes opératoires…). Un organisme peut librement adhérer à un code de conduite.
Le RGPD prévoit qu'un organisme tiers sera chargé de contrôler le respect d'un code, lui conférant un caractère contraignant.

MANDIL AVOCATS

MANDIL AVOCATS

Réaliser une analyse d'impact sur la vie privée

Fiche n°05 - Février 2020

Le RGPD prévoit la fin de la plupart des obligations en matière de formalités préalables (déclarations et autorisations de la CNIL). En contrepartie, le responsable de traitement doit être en mesure de démontrer à tout moment sa conformité aux exigences du RGPD (principe d'*accountability*).

Pour ce faire, il doit notamment mettre en place un registre des traitements et effectuer des analyses d'impact sur la vie privée (PIA – Privacy Impact Assessment), lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

A savoir — **L'obligation de tenir un registre des traitements de données**

Prévu à l'article 30 du RGPD, le registre participe à la documentation du traitement en permettant aux responsables du traitement et aux sous-traitants de recenser les traitements de données personnelles réalisés. Le registre détaille notamment les parties prenantes, les données traitées, l'utilisation et les destinataires des données, la durée de conservation et les mesures de sécurité.
Le registre est obligatoire pour entreprises de plus de 250 salariés et pour celles réalisant des traitements à titre régulier (gestion RH, prospection…). **En pratique, rares sont les entreprises dispensées de tenir un registre !**

I. Les traitements concernés

Les responsables de traitements effectuant des **traitements susceptibles de présenter un risque élevé** pour les droits et libertés des personnes concernées **sont tenus de réaliser des analyses d'impact** (article 35 du RGPD) lorsque le traitement :

OU

1. Remplit au moins 2 des critères suivants :

Réalisation d'évaluation ou de notation (profilage, scoring…)	**Surveillance/contrôle systématique des personnes concernées**
Traitement de **données sensibles** (origine ethnique, opinion politique, conviction religieuse, appartenance syndicale, donnée génétique ou biométrique) ou **hautement personnelles** (données de localisation, données financières…)	**Prise de décisions automatisées produisant des effets juridiques** ou affectant une personne de manière significative de façon similaire. Ex : rejet automatique et sans intervention humaine d'une demande de carte bancaire par le client d'un établissement bancaire...
Traitement des données à grande échelle (nombre de personnes concernées, volume de données, durée et étendue géographique)	**Traitement de données concernant des personnes vulnérables** (employés, enfants, malades mentaux, etc.).
Croisement de fichiers de données personnelles	**Usage innovant** (nouvelle technologie)

2. Figure sur la liste adoptée par la CNIL

- Traitements de **données de santé** par les établissements de santé ;
- Traitements de données **génétiques ou biométriques** de personnes dites « **vulnérables** » (patients, employés, enfants…) ;
- **Profilage** de personnes physiques à des fins RH ou **surveillance constante** de l'activité d'employés ;
- Traitements ayant pour finalité la gestion **des alertes et des signalements en matière sociale, sanitaire et professionnelle** ;
- Traitements impliquant le **profilage** des personnes pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci (**score pour l'octroi d'un crédit, LCLF aux moyens de paiement**…) ;
- Traitements de données de localisation à grande échelle ;
- …

II. Les traitements non concernés

Traitement ne présentant pas de risque élevé pour les droits et libertés des personnes concernées

Traitements figurant sur la liste des exceptions adoptée par la CNIL (gestion RH pour les petites sociétés, gestion des fournisseurs…)

Traitement nécessaire au respect d'une obligation légale ou nécessaire à l'exécution d'une mission d'intérêt public

Traitement (nature, contexte, finalité…) très semblable à un traitement ayant déjà fait l'objet d'une analyse d'impact

Les traitements initiés avant l'entrée en application du RGPD le 25 mai 2018 devront, s'ils se poursuivent, faire l'objet d'une analyse d'impact avant mai 2021 (et avant en cas de changement majeur affectant le traitement (nouvelle technologie…).

III. L'objet de l'analyse d'impact

L'analyse d'impact doit au moins contenir les éléments suivants :

Analyse d'impact

- **Description systématique** des opérations de traitement et des **finalités** du traitement
- **Evaluation juridique de la nécessité et de la proportionnalité** des opérations de traitement au regard des finalités
- **Etude technique des risques** pour les droits et libertés des personnes concernées (accès non autorisé, modification et disparition de données, et leurs impacts potentiels sur la vie privée)
- **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
- **Prise en compte de l'avis des personnes concernées** par les données (études, sondages ou enquêtes etc.) et/ou documentation de toute décision qui irait à l'encontre de l'avis reçu ou du non recueil de l'avis

IV. Qui intervient dans la réalisation de l'analyse ?

Intervenants

Juristes, métiers et RSSI du responsable du traitement

Délégué à la protection des données du responsable du traitement

Eventuels sous-traitants (assistance obligatoire)

A noter

Les outils pour réaliser une analyse d'impact

- Les lignes directrices du G29 sur les analyses d'impact du 4 octobre 2017
- Trois guides de la CNIL sur la méthodologie, l'outillage et bonnes pratiques
- Un logiciel libre de la CNIL permettant de réaliser des analyses d'impact
- La norme ISO/IEC 29134 «Privacy impact assessment – Guidelines»

V. L'avis de la CNIL

En cas de **risque élevé résiduel** qui n'a pas pu être suffisamment atténué par les mesures de sécurité prises suite à l'analyse d'impact (chiffrement, pseudonymisation…), le responsable du traitement devra **consulter la CNIL** avant de mettre en œuvre ce traitement (article 36 du RGPD). Il devra lui communiquer l'analyse d'impact effectuée.

La CNIL **rendra un avis** sous 8 semaines (+ 6 semaines en cas de traitement complexe) et **pourra s'opposer au traitement** à la lumière des caractéristiques et des conséquences du traitement sur les droits et libertés des personnes concernées par le traitement.

Deux régimes de formalités à réaliser auprès de la CNIL demeurent, pour des hypothèses très ciblées :

1. **Le régime de l'autorisation préalable pour :**
   - **Les traitements présentant une finalité d'intérêt public.**
   - **Les traitements automatisés dont la finalité est ou devient la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention.**
2. **Le régime de la demande d'avis sur un projet d'acte réglementaire autorisant un traitement de données de santé.**

MANDIL AVOCATS

MANDIL AVOCATS

Le Délégué à la protection des données

Fiche n°06 - Février 2020

Le RGPD crée la fonction de délégué à la protection des données (DPO) en remplacement de l'ancien Correspondant Informatique et Libertés (CIL).

Le DPO a vocation à agir en « Chef d'orchestre » en matière de traitement des données personnelles au sein de l'organisme qui l'a désigné et d'y piloter la conformité au RGPD des traitements de données personnelles réalisés.

A savoir

Quelles qualités pour le Délégué à la protection des données

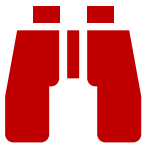
Le DPO peut être **interne ou externe**. Il peut être désigné pour plusieurs organismes sous conditions. Pour garantir l'effectivité de ses missions, le DPO :

- doit disposer de qualités professionnelles et de connaissances spécifiques (techniques et juridiques),
- doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement pour l'exercice de ses missions.

I. Quels organismes doivent désigner un DPO ?

Les autorités ou les organismes publics

Les organismes traitant à grande échelle des données relatives à des condamnations pénales et infractions



Les organismes traitant un suivi régulier et systématique des personnes à grande échelle

Tous les organismes privés, sur une base volontaire

II. Quelles sont les responsabilités & moyens d'action du DPO ?

1. Protection dans le cadre de ses fonctions

Le DPO est protégé par la règlementation européenne dans le cadre de l'exercice de ses fonctions :

- Il est soumis **à une obligation de confidentialité** en ce qui concerne l'exercice de ses missions.
- Il **n'est pas responsable en cas de de non-respect de la règlementation** par le responsable du traitement et / ou ses éventuels sous-traitant.

Toutefois, la responsabilité pénale du DPD peut être retenue s'il enfreint intentionnellement les dispositions du RGPD ou en tant que complice s'il aide le responsable du traitement et /ou le sous-traitant à enfreindre ces dispositions.

2. Moyens mis à sa disposition

L'organisme désignant le DPO devra :

Lui permettre d'agir de manière indépendante : positionnement hiérarchique adéquat, absence de conflit

S'assurer de son implication dans toutes les questions relatives à la protection des données **: communication interne et externe sur sa désignation…**

Lui fournir les ressources nécessaires à la réalisation de ses tâches : formation, temps nécessaire, ressources financières, équipe…

Lui faciliter l'accès aux données et aux opérations de traitement : accès facilité aux autres services de l'organisme…

III. Quelles sont les missions du DPO ?

1. Informer et conseiller

Le DPO doit informer et conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés au sujet des évolutions concernant la règlementation et formuler des recommandations à leur intention.

2. Assister le responsable de traitement lors de la réalisation des analyses d'impact

Le DPO donne son avis sur les questions suivantes :

- La nécessité ou non de procéder à une analyse d'impact relative à la protection des données ;
- La méthodologie à suivre lors de la réalisation d'une analyse d'impact relative à la protection des données ;
- Les mesures (y compris des mesures techniques et organisationnelles) à appliquer pour atténuer les risques éventuels pesant sur les droits et les intérêts des personnes concernées ;
- La question de savoir si l'analyse d'impact relative à la protection des données a été correctement réalisée et si ses conclusions (opportunité ou non de procéder au traitement et garanties à mettre en place) sont conformes aux exigences en matière de protection des données.

Lorsque le responsable du traitement est en désaccord avec l'avis fourni par le DPO, le responsable de traitement devra documenter et justifier les raisons pour lesquels il a passé outre cet avis.

3. Coopérer avec la CNIL et être le point de contact

Le DPO doit faciliter l'accès de la CNIL aux documents et informations de l'organisme (le registre par exemple) conformément aux missions et aux pouvoirs de CNIL.

Le DPO peut également entrer en contact avec la CNIL pour toute question relative à la conformité de l'organisme.

L'obligation de confidentialité ou de secret professionnel du DPO ne doit pas l'empêcher de demander conseil à l'autorité. Ses demandes seront traitées en priorité par la CNIL.

4. Contrôler le respect de la règlementation en matière de protection des données

Le DPO doit notamment :

- Recueillir des informations permettant de recenser les activités de traitement ;
- Analyser et vérifier la conformité de ces activités de traitement.

5. Aider à la tenue du registre

La tenue du registre incombe au responsable du traitement et aux sous-traitants. Le DPO peut toutefois se voir confier la mission de les aider à tenir le registre des opérations de traitement.

MANDIL AVOCATS

RGPD : comment protéger les droits des individus ?

Fiche n°07 - Février 2020

Le RGPD renforce les droits des personnes physiques concernées par un traitement de données personnelles.

Le fabricant d'un produit ou le concepteur d'un service doit veiller, dès la conception de ce produit/service, à ce que leurs utilisateurs, dont il obtiendrait des données personnelles, puissent exercer leurs droits de manière efficace… Sauf à anonymiser ces données de manière irréversible

A savoir — **Effectivité des droits et sous-traitants**

Les sous-traitants traitant des données personnelles pour le compte d'un responsable du traitement sont tenus d'aider ce dernier à garantir l'effectivité des droits des individus en mettant en place les mesures techniques et organisationnelles appropriées.
Il peut être décidé qu'ils gèrent eux-mêmes les demandes des individus s'agissant des données qu'ils traitent, ou qu'ils transmettent ces demandes au responsable du traitement.

I. Droit à la transparence

Préalablement à tout traitement de données personnelles, le responsable du traitement doit informer la personne concernée par le traitement :

- **Des mentions légales obligatoires** : identité du responsable de traitement, finalité du traitement, durée de conservation des données…
- **De ses droits** : d'accès, de rectification, d'opposition, à la portabilité, à la réparation des dommages matériel ou moral, ainsi qu'en cas de profilage…

A noter — **Une information claire, intelligible et aisément accessible**

- **Sur un site internet**, l'information doit figurer directement sur le formulaire de collecte et non dans les Conditions Générales d'Utilisation.
- **Dans un contrat**, ces informations doivent faire l'objet d'une clause spécifique.

II. Droit d'accès et de rectification

A la demande d'un individu, le responsable du traitement doit être en mesure de :

Communiquer à l'individu les données personnelles le concernant

Des frais raisonnables basés sur les coûts administratifs peuvent être prévus pour toute copie supplémentaire demandée.

Rectifier, supprimer ou mettre à jour les données personnelles inexactes

Des documents attestant de l'inexactitude des données peuvent être demandés à l'individu par le responsable du traitement.

III. Droit à la portabilité des données personnelles

A la demande d'un individu, le responsable du traitement doit être en mesure de transmettre les données personnelles le concernant :

- **A l'individu lui-même et / ou**
- **A un tiers** : un concurrent par exemple

Les données doivent être transmises dans un **format structuré, couramment utilisé et lisible par machine**.

! Le responsable de traitement ne sera pas automatiquement tenu de supprimer les données personnelles qu'il transmet.

Sont concernées

- **Données déclarées** activement et consciemment par la personne concernée (identité, coordonnées…)
- **Données attribuées** à la personne concernée ou générées par son activité (PAN, relevé de compte bancaire…)

Ne sont pas concernées

- **Données dérivées** où calculées à partir des données fournies (statistiques…)
- **Données traitées sur une autre base légale que le consentement ou l'exécution d'un contrat** : lutte contre le blanchiment, liste d'initiés, fichier incidents de paiement par carte…

IV. Droit d'opposition et de retrait du consentement

Ces droits dépendent de la base légale sur laquelle repose le traitement. Cf. Fiche n°03

Le responsable du traitement doit permettre à l'individu d'exercer son droit :

1. D'opposition, lorsque ce traitement est nécessaire :

A l'exercice d'une **mission d'intérêt public** ou est demandé par une **autorité publique**

OU

A un **intérêt légitime** du responsable du traitement (prospection, profilage, LCLF…)

En pratique

Le droit d'opposition a un effet rétroactif : le responsable de traitement devra mettre un terme au traitement **ET** supprimer ou **anonymiser** (de façon irréversible) les données personnelles déjà traitées dans un **délai de 1 mois**.

A noter

Refus de mise en œuvre du droit d'opposition

- S'il établit l'existence de **motifs impérieux et légitimes** justifiant le traitement et qui priment sur les intérêts ou les droits et les libertés de la personne concernée : le responsable du traitement pourra par exemple démontrer que les données sont nécessaires pour la lutte contre la fraude ou pour des raisons de sécurité…
- Si le traitement est nécessaire à une **action en justice**.

Il sera nécessaire de réaliser une véritable balance des intérêts.

2. De retirer son consentement

Le responsable du traitement doit permettre à un individu de **retirer son consentement à tout moment**.

En pratique

Ce droit ne s'applique que lorsque le traitement repose sur le consentement.

Le retrait du consentement n'a d'effet que pour l'avenir : le responsable du traitement doit simplement mettre un terme au traitement.
Ce droit s'applique indépendamment de celui à l'effacement.

! Lorsque le traitement repose sur **l'exécution d'un contrat**, l'opposition au traitement et le retrait du consentement ne sont pas possibles. Pour obtenir la fin d'un traitement de données personnelles, l'individu concerné devra **demander la résiliation du contrat selon les termes du contrat**.

V. Droit à l'effacement

Le responsable du traitement doit **assurer l'effacement des données personnelles** concernant un individu lorsque :

- Il n'y a **plus de raison de conserver** ces données : durée de conservation dépassée, objectif du traitement atteint…
- L'individu **s'oppose ou retire son consentement** au traitement
- L'individu **demande l'effacement** de données personnelles collectées lorsqu'il était mineur

VI. Droit à la limitation

Le responsable du traitement peut avoir à limiter le traitement de données personnelles à la demande d'un individu notamment lorsque :

- Une **demande de rectification des données ou d'opposition** a été effectuée et est en cours d'étude par le responsable de traitement.
- Les données personnelles **devraient être supprimées par le responsable de traitement** (Cf. droit à l'effacement) mais la personne concernée préfère qu'elles soient simplement conservées. Exemple : pour les besoins d'une action en justice.

VII. Intervention humaine

En cas de décision entièrement automatisée – y compris le profilage - ayant un effet juridique l'affectant, la personne concernée doit en être informé et peut demander l'**intervention d'un être humain qui puisse réexaminer la décision**.

VIII. Droit à la mort numérique

Il s'agit d'un droit prévu par la Loi de 1978. Le responsable du traitement doit permettre aux individus de leurs adresser des directives relatives à la **conservation, à l'effacement et à la communication de leurs données après leur décès.**

L'**exécuteur testamentaire et les héritiers** pourront demander l'application de ces directives par le responsable du traitement.

IX. Réclamation / réparation

La personne concernée a le droit de demander à tout moment :

Droit d'introduire une réclamation auprès d'une autorité de contrôle

Droit à réparation (responsabilité civile)

Action de groupe Droit de se faire représenter

MANDIL AVOCATS

MANDIL AVOCATS

Les violations de données personnelles

Fiche n°08 - Février 2020

Le RGPD impose aux entreprises qui traitent des données personnelles de mettre en œuvre des mesures globales de sécurité visant à :

- **prévenir toute violation de données personnelles ;**
- **mettre fin à la violation et minimiser ses effets ;**
- **Notifier les violations de données personnelles.**

A savoir

Qu'est-ce qu'une violation de données personnelles ?

Il s'agit d'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles, ou l'accès non autorisé à ces données. Exemples :

- suppression accidentelle de données bancaires ou de santé non sauvegardées par ailleurs ;
- perte d'une clef USB non sécurisée contenant une copie de la base clients d'une société ;
- introduction malveillante dans une base de données et modification des informations qui y sont stockées.

I. Prévenir et minimiser une violation de données personnelles

Les organismes qui traitent des données personnelles doivent mettre en œuvre des **mesures physiques, logiques et organisationnelles** appropriées de manière à prévenir les violations de données personnelles et à minimiser les effets de toute éventuelle violation :

1 **Certaines mesures concernent la sécurité des supports des traitements (matériels, logiciels, canaux de communication, supports papiers…) : gestion des accès, antivirus, sécurité des locaux, gouvernance…**

2 **D'autres mesures s'appliquent directement aux données traitées. Exemples :**

Anonymisation

Le recours (facultatif) à l'anonymisation irréversible des données permet de ne plus traiter de données personnelles. Pour cela :

- aucune mesure technique ne doit permettre de ré-identifier les individus ; ET
- il doit être impossible de déduire directement ou indirectement (via les données d'un tiers) l'identité d'un individu.

Exemples : altérer la véracité des données afin d'empêcher tout lien entre ces données et un individu, agréger les données de manière suffisamment importante…

Minimisation

Le RGPD prévoit que seules les données personnelles adéquates, pertinentes et limitées à ce qui est nécessaire pour atteindre les finalités prévues (LCLF, gestion du personnel…) doivent être collectées et conservées.

Exemples :

- ne pas collecter d'informations concernant les opinions politiques ou religieuses de clients dans un CRM.
- ne pas conserver 20 ans des données collectées uniquement à des fins de LCB/FT puisque l'obligation légale de les conserver n'est que de 5 ans.

Pseudonymisation

Le recours à la pseudonymisation doit être mis en œuvre dès que possible.

Cette mesure consiste à remplacer un attribut par un autre de telle façon que les données personnelles ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires.
L'identification indirecte est en théorie toujours possible mais le risque de mise en corrélation d'un ensemble de données avec un individu est réduit.

Exemples : chiffrement, hachage, tokenisation…

II. Notifier les violations de données personnelles

En cas de violation, le RGPD prévoit une notification sur trois niveaux qui dépend de la **gravité du risque pour les droits et libertés des personnes concernées** :

Pour les personnes concernées, la violation engendre :	aucun risque	un risque	un risque élevé
Documentation dans le registre interne des violations (à la disposition de la CNIL)	OUI	OUI	OUI
Notification à la CNIL, dans un délai maximal de 72h (motivation en cas de retard)	-	OUI	OUI
Information des personnes concernées (dans la mesure du possible de manière individuelle) dans les meilleurs délais	-	-	OUI

1. Comment apprécier l'absence de risque, le risque et le risque élevé ?

Cette appréciation doit être faite au cas par cas et doit tenir compte des éléments suivants :

- le type de violation (affectant l'intégrité, la confidentialité ou la disponibilité des données) ;
- la nature, la sensibilité et le volume des données personnelles concernées ;
- la facilité d'identifier les personnes touchées par la violation ;
- les conséquences possibles de celles-ci pour les personnes;
- les caractéristiques de ces personnes (enfants, personnes vulnérables, etc.) ;
- le volume de personnes concernées ;
- les caractéristiques du responsable du traitement (nature, rôle, activités).

Exemples de situations dans lesquelles il pourrait ne pas y avoir de risque justifiant une notification à la CNIL et / ou aux personnes concernées :

La divulgation de données déjà rendues publiques	La suppression de données sauvegardées et immédiatement restaurées
Des mots de passe d'employés ayant accès à une base de données sensibles ont été subtilisés, mais n'ont pas été utilisés et ont été réinitialisés	La perte de données protégées par un algorithme de chiffrement à l'état de l'art, si la clé de chiffrement n'est pas compromise et si une copie des données reste disponible

2. Quel est le point de départ du délai de notification

Le point de départ de la notification court dès lors que le responsable du traitement acquiert un degré de certitude raisonnable qu'un incident a eu lieu et a touché des données personnelles. Cela implique :

- Qu'il ait mis en place des mesures de détection des violations des données
- Qu'il mène au plus tôt des investigations permettant d'atteindre une telle certitude raisonnable

3. Quel est le rôle des sous-traitants en cas de violation de données ?

Le sous-traitant doit notifier au responsable du traitement toute violation de données **dans les meilleurs délais** après en avoir pris connaissance afin que le responsable du traitement puisse s'acquitter de ses obligations.

Le responsable du traitement peut également demander contractuellement au sous-traitant d'agir en son nom afin que ce dernier notifie directement la violation à la CNIL et aux personnes concernées.

MANDIL AVOCATS

Durée de conservation, archivage et anonymisation

Fiche n°09 - Février 2020

Les données personnelles ne peuvent pas être conservées indéfiniment. La détermination de leur durée de conservation dépend des objectifs du traitement et doit parfois tenir compte des éventuelles obligations légales de conserver et / ou d'archiver certaines données personnelles.

Lorsque la durée limite de conservation est atteinte et qu'il n'existe aucune raison d'archiver les données personnelles, celles-ci doivent être supprimées ou anonymisées de manière irréversible.

A savoir

Données personnelles et données anonymisées

Une donnée à caractère personnel est une information se rapportant à une **personne physique identifiée ou identifiable directement** (nom et prénom) **ou indirectement** (numéro de sécurité sociale, PAN, empreinte digitale...).

Une donnée anonymisée de manière irréversible n'est pas/plus une donnée personnelle. Dès lors, elle :

- Ne sera pas soumise aux dispositions du RGPD.
- Pourra être conservée indéfiniment.

I. Détermination de la durée de conservation

La durée de conservation d'une donnée personnelle dépend de la finalité de chaque traitement :

- Elle doit être déterminée par le responsable du traitement.
- **SAUF** lorsqu'elle est prévue par un texte législatif ou réglementaire. Dans ce cas, elle s'impose.

1. Détermination par le responsable du traitement

Les données personnelles doivent être conservées **uniquement le temps nécessaire à l'accomplissement de la finalité déterminée** lors de leur collecte.

EXEMPLE

Lors d'un achat sur internet, les coordonnées de la carte bancaire du client ne peuvent être conservées que le temps de réalisation de l'opération de paiement.

Toutefois, certaines de données personnelles (PAN et durée de validité) peuvent être conservées plus longtemps lorsqu'elles sont strictement nécessaires à d'autres finalités, comme par exemple :

- Pendant toute la durée d'exécution du contrat, lorsque ce dernier prévoit un abonnement impliquant des paiements multiples ;
- Pendant toute la durée d'inscription au service lorsque l'utilisateur a accepté que ses données personnelles soient conservées pour faciliter d'éventuels paiements ultérieurs ;
- Pendant une durée strictement nécessaire à la lutte contre la fraude au moyen de paiement.

2. Détermination par la Loi

Des dispositions légales et règlementaires définissent des **durées maximales de conservation** pour certains types de finalités.

EXEMPLES

- **Jusqu'à un mois** pour la conservation des images d'un dispositif de vidéosurveillance.
- **Jusqu'à 6 mois** concernant l'historique des connexions des salariés.
- **Jusqu'à 13 mois** pour les cookies déposés sur l'appareil de l'utilisateur d'un site internet.
- **Jusqu'à 3 ans** pour les coordonnées d'un prospect qui ne répond à aucune sollicitation pendant cette durée.
- **Jusqu'à 5 ans** pour les données personnelles nécessaires au contrôle des horaires des salariés.

II. Archivage

Lorsque les données personnelles ne sont plus nécessaires à la poursuite de la finalité pour laquelle elles ont été collectées, les données personnelles peuvent parfois être conservées dans une base d'archivage qui sera selon les cas intermédiaire ou définitive :

1. Archivage intermédiaire

De nombreuses dispositions légales prévoient une durée précise d'archivage de certaines données personnelles.
Seules les données absolument utiles au respect de l'obligation prévue devront être conservées.

EXEMPLES

- 5 ans pour les données relatives à gestion de la paie.
- 5 ans pour les contrats conclus entre commerçants ou entre commerçants et non-commerçants.
- 5 ans pour les informations nécessaires à la lutte contre le blanchiment et le financement du terrorisme.
- 10 ans pour les archives comptables et des pièces justificatives (factures…).

Il s'agit d'une durée minimale de conservation. Le responsable du traitement peut conserver les données plus longtemps si d'autres finalités déterminées et légitimes le nécessitent.

Pour faire valoir des droits en Justice.
Les données doivent être supprimées lorsque l'affaire a été jugée en dernier ressort ou lorsque l'action est prescrite.

EXEMPLE

Les données relatives aux cartes bancaires (hors cryptogramme visuel) peuvent être conservées en archivage intermédiaire pour une **finalité de preuve en cas d'éventuelle contestation de la transaction pour une durée de 13 mois.** Ce délai peut être étendu à 15 mois afin de prendre en compte la possibilité d'utilisation de cartes de paiement à débit différé.

2. Archivage définitif

Pour l'intérêt public.
Il est possible de conserver des données personnelles de **manière définitive** à des fins de recherche scientifique ou historique ou à des fins statistiques dans l'intérêt public.

La décision ainsi que les modalités d'archivage définitif des documents des collectivités « *sont définies par accord entre le service, l'établissement ou l'organisme intéressé et le service interministériel des Archives de France de la direction générale des patrimoines* » (article R. 212-13 du code du patrimoine).

Quelques règles à connaitre avant d'archiver des données personnelles

- Le **choix du mode d'archivage** est laissé à l'appréciation du responsable du traitement dès lors que les points ci-dessous sont respectés.
- **Des mesures techniques et organisationnelles** doivent être prévues pour protéger les données archivées de la destruction, de la perte ou de l'altération : gestion des accès et des habilitations aux seules personnes ayant un intérêt à accéder aux données, chiffrement…
- **Recours à un sous-traitant pour l'archivage** : le responsable du traitement doit s'assurer que son prestataire présente des garanties suffisantes en matière de sécurité et la confidentialité.
- **Protection des droits** : Une personne concernée par un traitement doit pouvoir exercer ses droits (d'accès, de rectification…) même lorsque les données sont archivées.

III. Suppression et anonymisation

Lorsque la durée limite de conservation est atteinte et / ou lorsqu'il n'y a plus de raison de les archiver, les données personnelles doivent obligatoirement être :

Définitivement et intégralement supprimées

OU

Anonymisées

L'anonymisation consiste à supprimer de façon irréversible tout lien permettant de rattacher les données personnelles traitées à une personne physique identifiée ou identifiable directement ou indirectement :

- A la différence de la pseudonymisation, **aucune mesure technique** ne doit permettre de ré-identifier les individus (absence de clé de déchiffrement…).
- La ré-identification doit également être **impossible par déduction** et au regard du contexte. En effet, quelques données « anonymes » peuvent parfois suffire à identifier formellement une personne, notamment lorsque le champ d'étude est restreint.

MANDIL AVOCATS

MANDIL AVOCATS

Les transferts de données personnelles hors de l'EEE

Fiche n°10 - Février 2020

La globalisation des échanges et l'utilisation croissante des nouvelles technologies ont conduit à un accroissement du nombre de transferts de données hors d'Europe.

Le RGPD encadre précisément ces transferts et il prévoit :

- **un principe d'interdiction des transferts de données personnelles hors de l'EEE (UE.**
- **de nombreuses exceptions à ce principe, complétées par le RGPD et plus ou moins faciles à utilisées.**

A savoir — **Extraterritorialité du RGPD**

Dans un contexte de mondialisation des échanges, le RGPD prévoit un principe d'extraterritorialité de la règlementation européenne qui s'applique à toutes les entreprises traitant des données personnelles de résidents européens (personnes présentes sur le territoire de l'UE au moment où le traitement est réalisé). Une entreprise traitant des données de résidents européennes à partir du sol des Etats-Unis devra donc, en théorie, appliquer le RGPD dès lors qu'elle cible les européens…

I. Les décisions d'adéquation

Le RGPD autorise les transferts vers les pays reconnus comme « adéquats » par la Commission européenne, c'est-à-dire dont la législation est jugée suffisamment protectrice.

L'adéquation peut être :

- **Totale** : c'est le cas des pays suivants : Argentine, Uruguay, Japon, Nouvelle Zélande, Suisse, Israël…
- **Partielle** : elle concerne uniquement les traitements réalisés dans un certain cadre, les autres transferts nécessitant d'être encadrés par d'autres outils.
  Exemples : transferts réalisés dans le cadre d'activités commerciales avec le Canada ou transferts vers les entreprises américaines ayant adhéré au **Privacy Shield**.

Le Privacy Shield fait suite à un premier accord UE-USA de 2000 (le Safe Harbor) invalidé par la CJUE en 2015.

Le PrivacyShield, permet à certaines entreprises de se conformer à un cadre juridique considéré comme suffisamment protecteur des données personnelles. Il prévoit notamment

- des droits pour les résidents européens (d'accès, d'opposition, de rectification, au recours…),
- des obligations pour les entreprises (principes de nécessité, de proportionnalité et de transparence…)
- un mécanisme de contrôle par les autorités américaines.

Concrètement, les entreprises souhaitant transférer des données personnelles depuis l'UE vers les États-Unis doivent s'engager à respecter ces dispositions pour être inscrites dans la liste des entreprises certifiées.

II. Les clauses contractuelles

Il s'agit de clauses de transfert de données personnelles destinées à être insérées par des responsables de traitements et / ou sous-traitants dans leurs contrats avec des prestataires extra-européens pour garanti la confidentialité et la sécurité des données personnelles qui lui sont communiquées.

Par ces clauses, l'importateur des données s'engage à assurer la confidentialité et la sécurité des données personnelles qui lui sont communiquées.

Il existe trois catégories de clauses :

Clauses contractuelles types adoptées par la Commission européenne

Clauses contractuelles types adoptées par une autorité de contrôle avec approbation de la Commission européenne

Clauses contractuelles spécifiques entre un organisme européen et un organisme extra-européen

Autorisation préalable de la CNIL nécessaire

Les transferts de données personnelles hors de l'EEE

III. Règles internes d'entreprise

Les *Binding Corporate Rules* (BCR) définissent la **politique d'une entreprise** en matière de transferts de données personnelles et **visent à assurer une protection adéquate aux données transférées** depuis l'Union européenne vers des pays tiers à l'Union européenne **au sein d'une même entreprise ou d'un même groupe**.

Les autorités européennes évaluent le contenu de chaque BCR pour s'assurer qu'il offre un niveau de protection adéquat aux données transférées en dehors de l'Union européenne.

Alternative aux CCT

- Uniformise les pratiques au sein d'un groupe
- Evite de conclure autant de contrats qu'il existe de transferts

IV. Outils normatifs

Les entreprises peuvent fonder leur transfert sur :

Un code de conduite approuvé par une autorité de contrôle

Un mécanisme de certification par une autorité de contrôle ou par un organisme de certification agréé par une autorité de contrôle ou un organisme national d'accréditation

Ces outils doivent être **assortis de l'engagement contraignant et exécutoire d'appliquer les garanties appropriées pour qu'une protection adéquate des données personnelles soit assurées**.

III. Des dispositions spécifiques

Des transferts de données personnelles hors EEE peuvent avoir lieu lorsque ils sont prévus par :

Des instruments juridiques contraignants entre autorités publiques (telle une convention internationale)

OU

Des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées

Autorisation préalable de la CNIL nécessaire

III. Situations particulières

Des transferts de données personnelles hors EEE peuvent avoir lieu lorsque le transfert est :

- Fondé sur le **consentement explicite et éclairé** ;
- **Nécessaire** à l'**exécution d'un contrat** ;
- **Nécessaire** pour des **motifs importants d'intérêt public**;
- **Nécessaire** à une **action en justice** ;
- **Nécessaire** à la **sauvegarde d'intérêts vitaux** ;
- **Réalisé au départ d'un registre** qui est légalement destiné à fournir des informations au public

Ces exceptions ne peuvent être interprétées que de **manière stricte** et ne s'appliquer que de manière **occasionnelle et ponctuelle** et en aucun cas pour des situations générales.

L'article 48 du RGPD conteste la possibilité pour un Etat non-membre de l'EEE de demander à une entreprise de lui transférer des données personnelles de résidents européens **sans accord international**.

Exemple : le Cloud Act ne pourra être opposé aux autorités européennes par les entreprises américaines exerçant des activités en Europe qu'à condition que des accords bi ou multilatéraux aient eu lieu entre des Etats membres européens et les Etats-Unis.

MANDIL AVOCATS

MANDIL AVOCATS

Sanctions en cas de violation du RGPD

Fiche n°11 - Février 2020

Le RGPD a renforcé le régime des sanctions applicables en cas de méconnaissance des dispositions en matière de protection des données personnelles. Elles doivent être proportionnées et dissuasives et peuvent consister en des amendes pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial...

Celles-ci peuvent survenir suite à une plainte et / ou une enquête de l'autorité de contrôle nationale ou dans le cadre de la coopération avec les autorités de contrôle européennes.

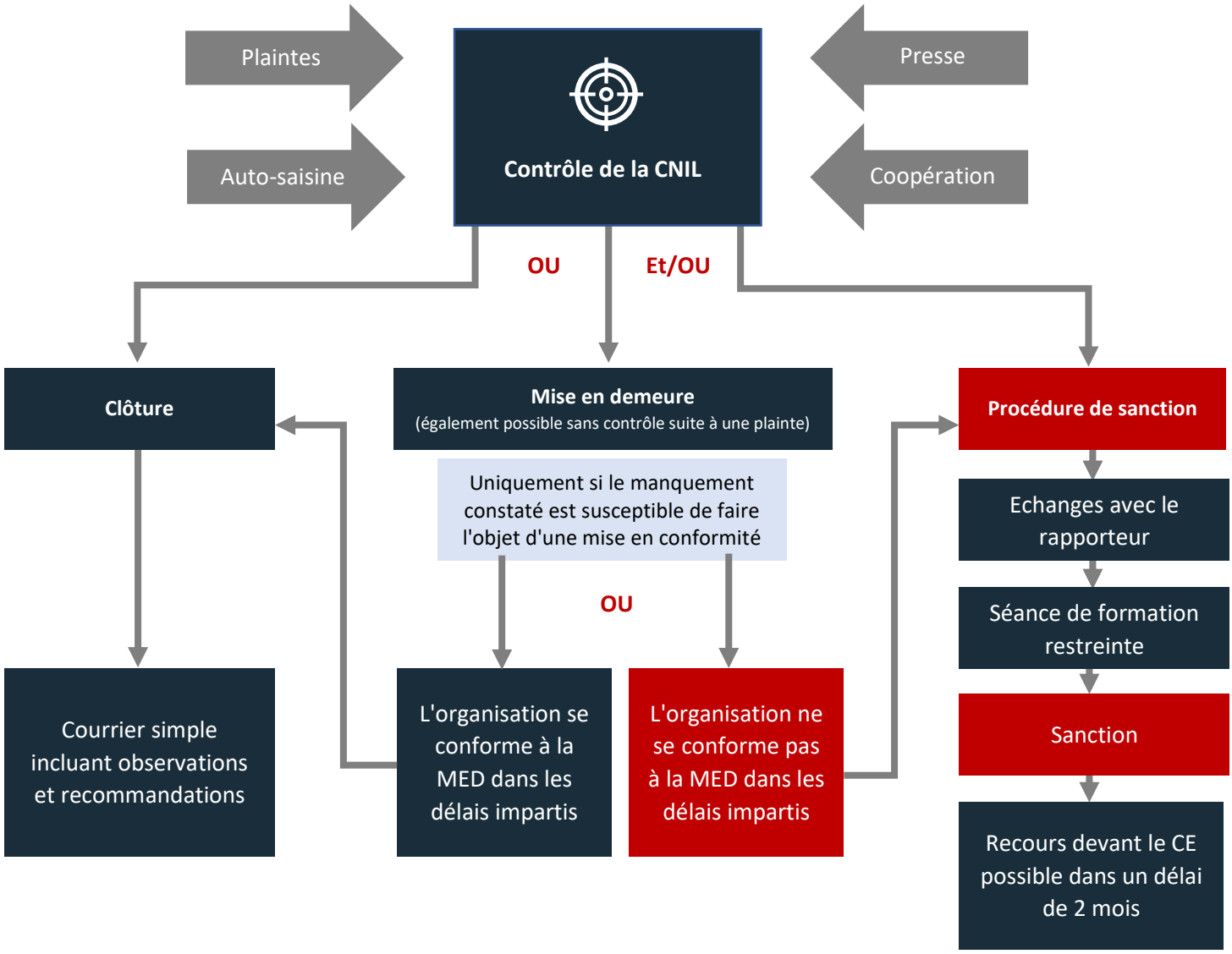
A savoir

Réclamation, recours juridictionnel et réparation

Les articles 77 et suivants du RGPD prévoient le droit pour toute personne :

- A un **recours juridictionnel effectif** en cas de violation de ses droits ;
- D'introduire une **réclamation** auprès d'une autorité de contrôle ;
- D'obtenir du responsable du traitement ou du sous-traitant **réparation du préjudice subi** du fait d'une violation du RGPD ;
- De **mandater un tiers** (organisme, association...) pour qu'il agisse en son nom (réclamation, demande de réparation...).

I. La procédure de sanction de la CNIL (schéma simplifié)



II. Les sanctions de la CNIL

En cas de manquement au RGPD ou à la loi « Informatique et Libertés », la formation restreinte de la CNIL peut prononcer les sanctions suivantes :

Rappel à l'ordre

Injonction de mettre en conformité le traitement ou de de satisfaire aux demandes d'exercice des droits
Astreinte de max 100K/jour

Interdiction ou limitation temporaire ou définitive du traitement

Retrait d'une certification

Suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale

Suspension partielle ou totale de la décision d'approbation des BCR

Amende administrative

→ **Jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial** en cas de non-respect des principes fondamentaux du RGPD, des droits des personnes, des dispositions sur les transferts ou de non-respect d'une injonction d'une autorité.

→ **Jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial** en cas de non-respect des obligations du responsable de traitement ou du sous-traitant (sécurité, analyse d'impact, tenue du registre, désignation d'un DPO...) ou de non-respect des obligations incombant à l'organisme de certification ou en charge des codes de conduite.

Publicité

→ La formation restreinte peut décider de **rendre publique** la décision qu'elle adopte et ordonner l'insertion de la décision dans des publications, journaux et supports qu'elle désigne, aux frais des organismes sanctionnés.

III. Autres conséquences d'un manquement

Sanctions pénales
(détournement de finalité, collecte par un moyen frauduleux, déloyal ou illicite, non-respect de l'opposition à de la prospection…)

Cinq ans d'emprisonnement et 300 000 euros d'amende (1.5 million pour une personne morale) !

Réparation civile
Articles 82 du RGPD et 1240 du Code civil

Responsabilité contractuelle
Non-respect des obligations contractuelles du sous-traitant ou du responsable conjoint du traitement…

Impact réputationnel
Perte de confiance des consommateurs / utilisateurs après une faille de sécurité, une mise en demeure ou une condamnation…

Tout responsable du traitement ayant participé un traitement méconnaissant les dispositions du RGPD sera responsable du dommage causé par celui-ci. Le sous-traitant ne sera responsable qu'en cas de non-respect des obligations qui lui incombent ou s'il a agi en-dehors des instructions licites du responsable du traitement. En cas de responsabilités multiples, la **responsabilité est solidaire avec action récursoire possible**.

MANDIL AVOCATS

MANDIL
AVOCATS

Besoin de fiches pratiques en droit du numérique adaptées à votre structure ou à votre activité ?

Contactez-nous !

11 Boulevard Sébastopol, 75001 PARIS

Tél. : +33 (0)9 53 17 44 88

contact@mandil-avocats.com