LES DOSSIERS TECHNIQUES

PRIVACY BY DESIGN / BY DEFAULT

Prise en compte de protection des données personnelles dès la conception et par défaut

Septembre 2022

CLUSIF

L’article L. 122-5 de la propriété intellectuelle n’autorisant pas les représentations ou reproduction intégrale, ou partielle, faite sans le consentement de l’auteur ou de l’ayant droit ou ayant cause, sauf exception stricte (« copies ou reproductions réalisées à partir d’une source licite et strictement réservées à l’usage privé du copiste et non destinées à une utilisation collective », analyses et les courtes citations dans un but d’exemple et d’illustration, etc.), toute représentation ou reproduction, par quelque procédé que ce soit du présent document sans autorisation préalable du Clusif constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Thomas	**VAN DEN HEUVEL**	Agence de la biomédecine

Les contributeurs :

Patrick	**BLUM**	Clusif
Fabrice	**IDIER**	Conseil départemental de la Seine Saint-Denis
Stéphanie	**JOUVE**	Médiane Systèmes
Fabrice	**POLLART**	Maisons & Cités
Frédéric	**VILANOVA**	Effective Yellow

Le Clusif remercie également les adhérents ayant participé à la relecture.

Introduction

Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données – RGPD) exige l'adoption de mesures techniques, juridiques et organisationnelles pour garantir la protection des données à caractère personnel. Il propose la prise en compte de ces exigences le plus en amont possible : on parle de protection des données dès la conception (*Privacy by Design*), de protection des données par défaut (*Privacy by default*). Par analogie, on peut parler également de sécurité dès la conception (*Security by design*).

En effet, s'il est nécessaire de garantir au quotidien l'existence et l'effectivité de mesures garantissant la protection des données à caractère personnel (on parlera dans ce document de « données personnelles »), il n'en reste pas moins que leur mise en œuvre est généralement beaucoup plus facile si la conception et le paramétrage initial de ces mesures ont été analysés, définis et mis en place au plus tôt dans le cycle de vie des projets et des activités d'une organisation.

Ce dispositif de protection des données dès la conception, par défaut et de sécurité par défaut s'inscrit donc :

- Lors de nouveaux projets et ce pour chaque traitement de données à caractère personnel ;
- Lors d'évolutions majeures de tout ou partie des traitements (maintenance, maintien en conditions opérationnelles…).

Le responsable de traitement[1] s'assure de l'adoption des règles internes et donne les moyens pour la mise en œuvre des mesures techniques et organisationnelles pour garantir cette protection.

Ce processus doit s'inscrire dans une démarche d'amélioration continue (*Plan Do Check Act*).

[1] https://clusif.fr/publications/faq-rgpd-donnees-a-caractere-personnel/

1 Définitions

1.1 Privacy by design / by default

1.1.1 Principes

Le CEPD/EDPS[2] (le DPO des institutions européennes) indique sur son site :

« *La protection des données par défaut est le principe selon lequel une organisation (le responsable du traitement) veille à ce que seules les données strictement nécessaires pour chaque objectif spécifique du traitement soient traitées par défaut (sans l'intervention de l'utilisateur). Afin de s'assurer que ce principe clé du règlement général sur la protection des données est mis en pratique, le CEPD publiera des documents d'orientation.* » [3]

« *Les entreprises/organisations sont encouragées à mettre en œuvre des mesures techniques et organisationnelles dès les premières étapes de la conception des opérations de traitement, de manière à préserver dès le départ la vie privée et les principes en matière de protection des données (« protection des données dès la conception »). Par défaut, les entreprises/organisations doivent s'assurer que les données à caractère personnel sont traitées selon le niveau le plus élevé de protection de la vie privée (par exemple, seules les données nécessaires devraient être traitées, une durée de conservation brève et une accessibilité limitée) afin que, par défaut, les données à caractère personnel ne soient pas rendues accessibles à un nombre indéterminé de personnes (« protection des données par défaut»).* » [4]

1.1.2 Définitions

Il ressort du RGPD (*article 25*) :

- *Privacy by Design* (protection des données dès la conception)

La protection des données dès la conception vise à intégrer la protection des données et le respect de la vie privée dans la conception des activités de traitement et des systèmes d'information, afin de respecter les principes de protection des données.

- *Privacy by Default* (protection des données par défaut)

La protection des données par défaut est le principe selon lequel une organisation (le responsable du traitement) veille à ce que seules les données strictement nécessaires pour chaque objectif spécifique du traitement soient traitées par défaut (sans l'intervention de l'utilisateur).

1.2 « Security by design / by default »

Par analogie avec les concepts de *privacy by design / by default*, on parle de *security by design / by default* qui correspond aux mesures de sécurité encadrant les traitements de données personnelles.

---

[2] Comité européen de protection des données. Le Comité européen de la protection des données (EDPB) est un organe européen indépendant qui contribue à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne et encourage la coopération entre autorités de l'UE chargées de la protection des données.

[3] https://edps.europa.eu/data-protection/our-work/subjects/protection-des-donnees-par-defaut_fr

[4] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_fr

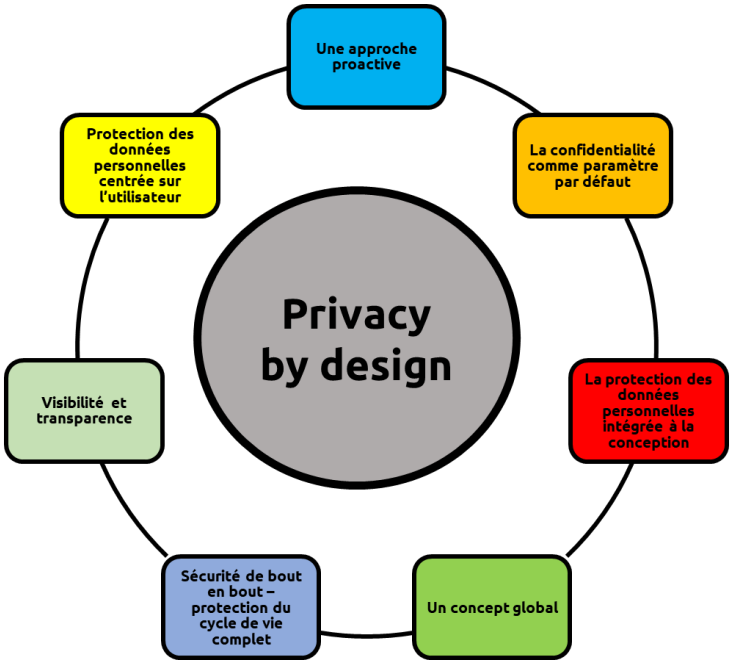
Les concepts de « *security by design* » (intégration de la sécurité dès la conception d'un système) et de « *security by default* » (système sécurisé par défaut, sans nécessité de paramétrage complémentaire) sont désormais primordiaux au regard de l'augmentation des cyberattaques, opportunistes ou ciblées, pour limiter les coûts et efforts nécessaires à la sécurisation d'un SI *a posteriori* [5].

[5] Note blanche ANSSI 10/08/2021 : système d'information hybride et sécurité : un retour à la réalité https://www.ssi.gouv.fr/uploads/2021/08/anssi-article-systemes_information_hybrides_et_securite_un_retour_a_la_realite.pdf

2 Principes du « Privacy by Design »

2.1 Sept principes fondamentaux

Toute conception implique avant tout de respecter les principes du RGPD détaillés ci-après.



Le concept de *Privacy by Design* repose sur sept principes fondamentaux, et représente une solution permettant aux technologies d'évoluer dans une coexistence saine et pérenne du numérique et des individus sans porter atteinte à la vie privée des individus dont les données personnelles sont collectées et utilisées.

2.1.1 Une approche proactive

L'approche *Privacy by Design* se caractérise par des mesures proactives. Cette approche cherche à anticiper et prévenir les événements portant atteinte à la protection des données avant qu'ils ne se produisent.

Cette approche constante dans cette démarche s'applique notamment aux technologies de l'information, aux pratiques organisationnelles, aux écosystèmes d'information en réseau.

Cela implique :

- Un engagement clair au plus haut niveau pour fixer et appliquer des normes élevées en matière de protection des données personnelles ;
- Un engagement en faveur de la protection des données manifestement partagé par les responsables des traitements impliqués dans le projet, les personnes chargées de la mise en œuvre, les utilisateurs internes et externes, y compris les prestataires éventuels ;
- Des points de contrôle visant à identifier et corriger les mauvaises pratiques en matière de protection des données personnelles à chaque étape clé du projet.

Exemples : cahier des charges, recettes, mesures techniques, juridiques et organisationnelles, étude d'impact sur la vie privée des personnes si nécessaire…

2.1.2 La confidentialité comme paramètre par défaut

Le principe du *Privacy by Design* vise à garantir un niveau maximal de protection dès la conception des traitements des données personnelles du projet en veillant à ce que les données soient protégées.

Il appartient au responsable de traitement de définir et mettre en œuvre les mesures de protection adéquates.

2.1.3 La protection des données personnelles intégrée à la conception

La protection des données personnelles est un élément essentiel de la fonctionnalité de base fournie. La protection des données personnelles fait partie intégrante de la conception du système, sans en diminuer la fonctionnalité.

La protection des données personnelles doit être intégrée aux technologies, aux opérations et aux architectures d'information en tenant compte notamment du contexte et des parties prenantes.

- Il convient d'adopter une approche systémique, fondée sur des principes, pouvant s'appuyer sur des normes et cadres permettant d'être audités ;
- Des études d'impact sur la protection des données personnelles sont parfois nécessaires pour évaluer les risques d'atteinte à la protection des données ;
- Les mesures qui en résultent, définies dans un plan d'actions, doivent permettre de réduire au minimum les risques d'une mauvaise utilisation, d'une mauvaise configuration ou d'une erreur. Le responsable de traitement peut alors accepter ou non les risques résiduels, sous réserve de s'assurer de la conformité du traitement de données personnelles à la réglementation applicable.

2.1.4 Un concept global

Le principe du *Privacy by Design* vise à rechercher un équilibre entre respect de la vie privée et utilisation optimale des services numériques ouverts aux usagers d'une part, et à prendre en compte tous les intérêts et objectifs légitimes d'une manière positive, alliant protection des données personnelles et sécurité d'autre part.

Les objectifs du traitement, les fonctions annoncées, les mesures convenues et appliquées doivent être clairement documentés.

2.1.5 Sécurité de bout en bout - protection du cycle de vie complet

Le *Privacy by Design* s'étend à l'ensemble du cycle de vie des données concernées.

De solides mesures de sécurité sont essentielles à la protection des données personnelles, du début à la fin du traitement, afin de garantir que toutes les données soient conservées, archivées puis éventuellement détruites, en toute sécurité du début à la fin du traitement.

Ainsi, le processus *Privacy by Design* garantit une gestion sécurisée du cycle de vie des informations, de bout en bout. Sans garantie de la sécurité, il ne peut y avoir de protection des données personnelles.

Les normes de sécurité appliquées doivent garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données personnelles tout au long de leur cycle de vie, notamment des méthodes de destruction sécurisée, un chiffrement approprié, des méthodes de contrôle d'accès et de journalisation solides.

2.1.6 Visibilité et transparence

Le principe de *Privacy by Design* vise à garantir à toutes les parties prenantes que, quelle que soit la pratique commerciale ou la technologie concernée, celle-ci fonctionne effectivement conformément aux engagements et aux objectifs énoncés. Les composants et leurs opérations du traitement doivent rester visibles et transparents pour les utilisateurs et les fournisseurs.

La visibilité et la transparence sont essentielles pour établir la confiance.

- **Responsabilité :** La collecte d'informations personnelles entraîne un devoir de diligence pour leur protection. La responsabilité de la rédaction et de l'approbation des politiques et des procédures de la protection des données personnelles doit être documentée et communiquée. Une responsabilité doit être attribuée à une personne déterminée. En cas de transfert de données personnelles à des tiers, une protection équivalente des données personnelles doit être assurée par des moyens contractuels. [6] [7]
- **Ouverture :** L'ouverture et la transparence sont les clés de la responsabilité. Les informations sur les politiques et pratiques relatives à la gestion des données personnelles doivent être facilement accessibles aux personnes concernées.
- **Conformité :** Des mécanismes de plainte ou de réclamations doivent être mis en place et facilités par une communication adaptée.

Des mesures doivent être prises pour contrôler, évaluer et vérifier la conformité aux politiques et procédures de protection des données personnelles.

2.1.7 Protection des données personnelles centrée sur l'utilisateur

Les meilleurs résultats en matière de *Privacy by Design* sont généralement ceux qui sont consciemment conçus autour des intérêts et des besoins des utilisateurs individuels, devant être en capacité de gérer leurs propres données personnelles.

Donner aux personnes concernées le pouvoir de jouer un rôle actif dans la gestion de leurs propres données est souvent le moyen le plus efficace de lutter contre les abus et les mauvaises utilisations.

La protection des données personnelles des utilisateurs s'appuie sur :

- **L'une des bases légales prévues par le RGPD** : La collecte, l'utilisation ou la divulgation des données personnelles doivent respecter l'une des six conditions de licéité prévues par l'article 6 du RGPD : exécution d'un contrat, respect d'une obligation légale, sauvegarde d'intérêts vitaux, mission d'intérêt public, intérêt légitime du responsable de traitement, consentement de la personne ;[8]
- **Information :** L'utilisateur doit être prévenu par des mentions légales des caractéristiques du traitement (finalité, exercice des droits, réclamation) ;
- **Consentement :** Dans le cas particulier du consentement, celui-ci doit être libre et spécifique pour la collecte, l'utilisation ou la divulgation d'informations personnelles. Plus la sensibilité des données est grande, plus la qualité du consentement requis doit être claire et spécifique. Le consentement peut être retiré à une date ultérieure ;[9]
- **Exactitude :** les données personnelles doivent être aussi exactes, complètes et à jour que nécessaire pour atteindre les objectifs spécifiés ;
- Principes de **loyauté, proportionnalité et minimisation** ;
- **Accès :** Les personnes doivent pouvoir obtenir un accès à leurs données personnelles et être informées de leurs utilisations et divulgations. Les personnes doivent pouvoir

[6] https://clusif.fr/publications/responsabilite-des-sous-traitants/

[7] https://clusif.fr/publications/les-reglementations-liees-a-la-protection-des-dcp/

[8] https://clusif.fr/publications/faq-rgpd-quels-sont-les-principes-du-reglement/

[9] https://clusif.fr/publications/faq-le-consentement-au-traitement-des-donnees-personnelles/

contester l'exactitude et l'exhaustivité des informations et les faire modifier le cas échéant, sous réserve que cela soit légitime ; [10]

- **Conformité :** En plus d'avoir informé les personnes des collectes et traitements mis en place, les organisations doivent prévoir des mécanismes de plainte et de réclamation et communiquer au public des informations à leur sujet, notamment sur la manière d'escalader en cas de besoin.

Il importe de mettre en œuvre des mécanismes robustes et fiables qui permettent aux personnes concernées d'exercer leurs droits en matière de protection des données.

Le respect des données personnelles des utilisateurs s'étend à la nécessité pour les interfaces homme-machine d'être centrées sur l'homme, centrées sur l'utilisateur afin que des décisions éclairées en matière de protection des données personnelles puissent être prises de manière fiable. De même, les opérations commerciales et les architectures physiques impliquées dans la collecte des données personnelles doivent faire preuve du même degré de considération pour l'individu.

- https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
- https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/

2.2 Finalité du traitement[11]

Les données sont recueillies et collectées pour des finalités déterminées, explicites et légitimes. Elles ne sont pas traitées ultérieurement de manière incompatible avec ces finalités (article 5 du RGPD).

En cas de changement de finalité, le règlement pose le principe de l'exigence de la compatibilité des finalités nouvelles avec les finalités initiales, sauf consentement de la personne concernée ou lorsqu'un texte légal spécifique le permet. En cas d'incompatibilité, la poursuite de la finalité incompatible est proscrite.

2.2.1 Objectif de la collecte

Il importe de définir l'objectif poursuivi par la mise en place d'un traitement de données. Cet objectif doit être compatible avec les missions de l'organisme. Il doit être clair et compréhensible pour les personnes concernées.

En fonction, les données collectées ne peuvent pas être utilisées pour un autre objectif que celui qui a été défini.

Exemples de finalités : gestion du recrutement, gestion de la clientèle, enquête de satisfaction, protection des biens et des personnes, etc.

Si une modification ou un ajout d'objectif relatif à un traitement de données personnelles survient, ce changement doit être clairement documenté. Il doit être communicable de façon compréhensible par les personnes concernées par le traitement.

2.2.2 Base légale de traitement

La base légale sur laquelle repose le traitement de données mis en œuvre a été identifiée.

Selon l'article 6 du règlement européen, pour être licite, un traitement de données doit être fondé sur l'une des bases légales suivantes : exécution d'un contrat, obligation légale, sauvegarde des intérêts vitaux, mission d'intérêt public, intérêts légitimes ou consentement de la personne concernée.

[10] https://clusif.fr/publications/faq-rgpd-exercice-des-droits-des-personnes/

[11] https://clusif.fr/publications/faq-rgpd-quels-sont-les-principes-du-reglement/
https://clusif.fr/publications/faq-rgpd-quelles-sont-les-obligations-du-responsable-de-traitement-rt/

2.3 Données traitées

2.3.1 Catégories de données

Les catégories de données pouvant alimenter le traitement ont été identifiées en amont, y compris les catégories particulières de données et les données relatives à des condamnations ou à des infractions, définies par les articles 9 et 10 du RGPD, couramment appelées « données sensibles ».

Les traitements des catégories particulières de données (qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques, les données concernant la santé, les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique) sont par principe interdits. L'utilisation de ces données est strictement encadrée par la réglementation (RGPD, loi Informatique et Libertés, réglementation spécifique applicable…)[12]. Il importe dans chaque organisation de se rapprocher du délégué à la protection des données (DPD ou DPO).

Types de données	Catégories de données
DCP courantes	Etat-civil, identité, données d'identification
	Vie personnelle (habitudes de vie, situation familiale, hors données sensibles)
	Vie professionnelle (CV, scolarité, formation professionnelle, distinctions…)
	Informations d'ordre économique et financier (revenus, situation financière, situation fiscale…)
	Données de connexion (adresses IP, journaux d'évènements…)
	Données de localisation (déplacements, données GPS, GSM…)
DCP perçues comme « sensibles »	Numéro de sécurité sociale (NIR)
	Données biométriques (dont images et voix)
	Données bancaires
DCP « sensibles » au sens du règlement	Origines raciales ou ethniques, opinions politiques, convictions philosophiques ou religieuses, appartenance syndicale, données concernant la vie sexuelle ou l'orientation sexuelle de la personne concernée, données de santé, données génétiques, données biométriques.
	Infractions, condamnations, mesures de sûreté
	Données concernant les mineurs

Tableau 1 : principales catégories de données à caractère personnel

2.3.2 Origine des données

L'origine des données a été identifiée pour chaque collecte (collecte directe auprès de la personne ou indirecte auprès de tiers).

Par exemple - collecte indirecte - des cookies installés sur le terminal de connexion de l'utilisateur

2.3.3 Minimisation des données

Les données collectées pour le traitement sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard de l'objectif pour lequel elles ont été collectées (article 5 du RGPD).

[12] https://clusif.fr/publications/faq-rgpd-donnees-a-caractere-personnel/

Seules les données adéquates et strictement nécessaires à la finalité du traitement sont autorisées à y figurer.

Par exemple, il n'est pas pertinent de demander la date de naissance d'un client pour alimenter un fichier dont la finalité est la gestion des achats d'un magasin de meubles.

2.4 Durée de conservation et Archivage des données personnelles

2.4.1 Durée de conservation

Le traitement mis en œuvre doit permettre de gérer les durées de conservation et la suppression en adéquation avec la spécificité des données faisant l'objet du traitement.

Selon l'article 5e du RGPD, les données personnelles 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.

La définition de la durée de conservation relève de l'analyse de conformité que le responsable doit mener pour son traitement. Dans certains cas, la durée de conservation est fixée par la règlementation (par exemple, l'article L3243-4 du Code du travail impose à l'employeur de conserver un double du bulletin de paie du salarié pendant 5 ans). Toutefois, pour de nombreux traitements de données, la durée de conservation n'est pas fixée par un texte. Il appartient alors au responsable du fichier de la déterminer en fonction de la finalité du traitement.

Les données à caractère personnel peuvent toutefois être conservées pour des durées plus longues :

- Dans la mesure où elles seront **traitées exclusivement à des fins archivistiques**, y compris dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ;
- Dans le cas où elles ont fait l'objet d'une **anonymisation** conformément aux recommandations de la CNIL : elles ne sont plus considérées comme des données à caractère personnel et ne sont plus soumises au RGPD. Mais l'anonymisation véritable est très difficile car il s'avère dans les faits qu'il est presque toujours possible de réidentifier la personne concernée en croisant des informations ou par connaissance du domaine.

2.4.2 Archivage des données

Le traitement permet de séparer logiquement les données archivées des données opérationnelles, de restreindre l'accès aux informations archivées *via* des procédures d'habilitation particulières et de vérifier la traçabilité des consultations.

Pour un même traitement, les données personnelles poursuivent des phases successives. On parle de « cycle de vie » de la donnée personnelle.

Ce cycle connaît trois phases :

- **Conservation en base active** (autrement appelée « archives courantes ») : Il s'agit de la durée nécessaire à la réalisation de l'objectif (finalité du traitement) ayant justifié la collecte/enregistrement des données. En pratique, les données seront alors facilement accessibles dans l'environnement de travail immédiat pour les services opérationnels qui sont en charge de ce traitement (ex : le service des ressources humaines pour les opérations de recrutement).

- Les **archives intermédiaires** (impliquant un accès restreint, il s'agit d'une étape intermédiaire avant la suppression ou l'anonymisation des données) : Les données personnelles ne sont plus utilisées pour atteindre l'objectif fixé (« dossiers clos ») mais

présentent encore un intérêt administratif pour l'organisme (ex : gestion d'un éventuel contentieux, etc.) ou doivent être conservées pour répondre à une obligation légale (par exemple, les données de facturation doivent être conservées dix ans en application du code de commerce, même si la personne concernée n'est plus cliente). Les données peuvent alors être consultées de manière ponctuelle et motivée par des personnes spécifiquement habilitées.

- Les **archives définitives** (données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction) : En raison de leur « valeur » et intérêt, certaines informations sont archivées de manière définitive et pérenne.

À la différence de la conservation en base active, les deux dernières étapes ne sont pas systématiquement mises en place. Leur nécessité doit être évaluée pour chaque traitement, et, pour chacune de ces phases, un tri sera opéré entre les données.

2.5 Zones de libre commentaire ou données non structurées

Lorsque des zones de commentaires sont présentes ou lorsqu'il existe des données non structurées (par exemple des photos, images, vidéos), leur utilisation est strictement encadrée par l'organisation pour éviter que ces espaces puissent porter atteinte aux droits des personnes concernées. Il est donc nécessaire d'effectuer des audits réguliers pour garantir la conformité des données saisies.

Les informations saisies dans les zones libres (commentaires) font partie des données qui seront communiquées à la personne concernée si celle-ci exerce son droit d'accès.

Il peut être utile de le rappeler aux opérateurs par des programmes de sensibilisation, des messages d'alertes au moment de la saisie.

D'autres mesures techniques peuvent bloquer la saisie de mots interdits ou au contraire limiter la saisie par une liste de mots autorisés.

2.6 Consentement

Le consentement est l'une des bases légales, ou conditions de licéité, prévues par le règlement européen sur laquelle peut se fonder un traitement de données à caractère personnel. Le RGPD impose que ce consentement soit libre, spécifique, éclairé et univoque (RGPD, Art. 4 et 7). Le consentement de la personne concernée est défini par le règlement européen 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* » (RGPD, Art. 4 11°).

Dans le cas où un traitement de données personnelles mis en œuvre a pour base légale le consentement en application de l'article 6 du RGPD, le responsable de traitement doit être en mesure de démontrer que la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement de données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par moyen électronique.[13]

Le règlement ne précise pas de durée spécifique du consentement. La durée de validité du consentement dépendra du contexte, de la portée du consentement initial et des attentes de la personne concernée.

[13] https://clusif.fr/publications/faq-rgpd-exercice-des-droits-des-personnes/

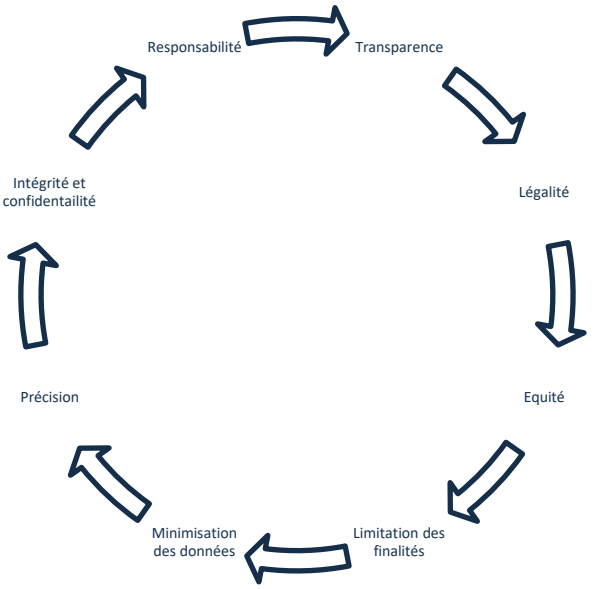
Le CEPD recommande, à titre de bonne pratique, que le consentement soit renouvelé à des intervalles appropriés.

Les personnes concernées par le traitement des données ont reçu lors de la collecte de leurs données, par écrit ou par d'autres moyens, une information suffisante, transparente, compréhensible et aisément accessible.

Par exemple : Conditions Générales d'Utilisation (CGU), mentions sur les formulaires de collecte, icônes, mentions légales etc.

Le responsable du traitement doit fournir à la personne concernée toute autre information nécessaire pour garantir un traitement équitable et transparent, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées (*RGPD, considérant 60*).

Conformément à l'article 12 du règlement, l'information des personnes est une exigence règlementaire obligatoire, qui rejoint le cadre général de *l'Accountability* (responsabilité) imposant une transparence renforcée concernant les traitements de données. Les mentions d'informations doivent comporter l'ensemble des éléments mentionnés aux articles 13 et 14 du règlement européen.



Le règlement accorde par ailleurs une place importante au retrait du consentement. L'article 7 précise que la personne a le droit de retirer son consentement à tout moment. Pour lui, retirer son consentement doit être aussi simple que de le donner, sans préciser si la personne concernée doit toujours pouvoir donner et retirer son consentement moyennant la même action.

Le responsable de traitement doit alors supprimer les données ayant été traitées sur la base du consentement une fois le consentement retiré, à la condition qu'aucune autre condition de licéité ne justifie leur conservation.

2.7 Gestion de droits des personnes[14]

L'article 12 du règlement impose au responsable de traitement de mettre en place des procédures internes assurant le respect des différents droits alloués aux personnes concernées par les traitements de données. La mise en œuvre et le maintien en conformité à la règlementation européenne nécessitent la mise en place des processus pour répondre aux droits des personnes (demandes de droit d'accès, de rectification, d'opposition, limitation, portabilité, oubli).

[14] https://clusif.fr/publications/faq-rgpd-exercice-des-droits-des-personnes/

Le responsable de traitement (RT) doit en effet faciliter l'exercice des droits conférés à la personne (*RGPD, Art.12, C59*)[1]. Le règlement évoque notamment la possibilité de fournir les moyens aux personnes de présenter leurs demandes par voie électronique. Le RT doit répondre dans les meilleurs délais et *en tout état de cause, dans un délai d'un mois à compter de la réception de la demande*. Au besoin, ce délai peut être porté à 2 mois au regard de la complexité et du nombre de demandes. Le responsable de traitement doit alors informer le demandeur de la prolongation du délai pour répondre et indiquer les motifs de ce report.

Ces procédures internes doivent prévoir pour le(s) traitement(s) mis en œuvre, la méthode par laquelle les personnes peuvent exercer leurs droits, le service ou la personne chargé(e) de répondre et la forme par laquelle sera transmise la réponse. Si le RT ne donne pas suite à la demande formulée, il doit informer la personne et motiver sa réponse. Il doit également indiquer la possibilité pour la personne d'introduire une réclamation auprès de l'autorité de contrôle (la CNIL en France, *RGPD, Art.12*).

2.8 Analyse de conformité technique / Sécurité du traitement de données[15]

2.8.1 Mise en place des mesures de protection

En application de l'article 32§2 du règlement[16], le responsable du traitement ou le sous-traitant doit évaluer les risques inhérents au traitement afin d'identifier les risques que présente le traitement et mettre en œuvre les mesures techniques et organisationnelles adaptées pour les réduire.

Les mesures techniques et organisationnelles mises en œuvre pour assurer la sécurité du traitement des données doivent tenir compte de l'état de l'art, de la probabilité et de la gravité du risque pour les personnes concernées.

Par exemple :

- La pseudonymisation (anonymisation réversible) 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.

2.8.2 Traitements à risque

Le règlement identifie un certain nombre de traitements susceptibles de présenter un risque plus élevé pour la protection de la vie privée qui pourront nécessiter la réalisation d'une analyse d'impact.

Ce sont en particulier :

- Les traitements de données à caractère personnel considérées comme sensibles (données de santé, opinions politiques, vie sexuelle, origine ethnique ou raciale, biométrie, génétique, données de mineurs, personnes vulnérables etc.)
- Les traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques » (article 35 du RGPD), notamment de profilage (*scoring*, capacité au crédit, localisation, comportement...)

[15] https://clusif.fr/publications/faq-rgpd-analyse-dimpact-pia/

[16] https://clusif.fr/publications/faq-rgpd-donnees-a-caractere-personnel/

- Les systèmes de surveillance (vidéo, drones, robots etc.)

2.8.3 Analyse d'impact sur la protection des données

Préalablement à la mise en œuvre du traitement, il est nécessaire de mener une analyse de risques résiduels afin d'identifier un niveau de sécurité considéré comme suffisant par la règlementation européenne.

L'analyse d'impact relative à la protection des données (AIPD ou DPIA en anglais) est réalisée pour le traitement lorsque celui-ci est susceptible de présenter des "risques élevés" pour les droits et libertés des personnes physiques.

Selon l'article 35 du RGPD, pour tous les traitements à risque, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées.

2.9 Sécurité des données

S'il importe d'assurer la sécurisation des données personnelles traitées dans toutes les opérations du traitement de données, il en va particulièrement lorsque ces données font l'objet d'un transfert vers des tiers, la sécurisation des données devant alors en particulier être prévue, notamment via une convention spécifique mentionnant les obligations de chacune des parties, que ce soit vers un prestataire situé au sein de l'Union européenne ou en dehors de l'Union européenne.

Exemples : Chiffrement de données, chiffrement du canal de transmission lors d'un envoi via un réseau, un portail sécurisé, sous la forme d'un service Web associé à l'utilisation de certificats.

Une attention particulière doit être portée sur la transmission par email.

Par exemple : pas d'envoi de bulletin de salaire en format pdf non chiffré par messagerie non chiffrée.

2.9.1 Chiffrement des données

Dans certaines circonstances (par ex : envoi de données personnelles par mail), il peut être nécessaire de chiffrer les données. Il convient donc :

- d'identifier les données concernées ;
- de prévoir des mesures particulières à adapter aux circonstances : chiffrement des données (brutes, en base, des sauvegardes)…

2.9.2 Authentification renforcée

La politique de gestion des mots de passe et d'authentification forte mise en œuvre est conforme aux recommandations de l'ANSSI et de la CNIL.

Les exigences minimales de la CNIL et de l'ANSSI en termes de taille et de complexité du mot de passe varient en fonction des mesures complémentaires mises en place pour fiabiliser le processus d'authentification : ainsi, si une authentification est basée exclusivement sur un mot de passe, cela implique *à minima* l'utilisation d'un mot de passe complexe d'au moins 12 caractères composé de majuscules de minuscules, de chiffres et de caractères spéciaux.

Des mesures complémentaires à la saisie d'un mot de passe (restrictions d'accès, collecte d'autres données, support détenu en propre par l'utilisateur) permettent de réduire la longueur et la complexité du mot de passe, car ces mesures permettent d'assurer un niveau de sécurité équivalent au mot de passe seul.

Une authentification forte est privilégiée nécessitant l'utilisation de deux facteurs différents.

Une authentification multi facteurs permet de prouver l'identité d'un utilisateur par la vérification de plusieurs éléments, appelés facteurs d'authentification.

Chacun des facteurs d'authentification mis en œuvre doit appartenir à une catégorie de facteur différente :

- Facteur de connaissance (mot de passe, code…) ;
- Facteur de possession (token, smartphone…) ;
- Facteur inhérent (empreinte digitale, voix...).

L'absence d'un des facteurs nécessaires à une authentification multi facteur doit faire échouer l'authentification.

2.9.3 Gestion des habilitations

Les collaborateurs internes ayant accès aux données traitées ont été clairement identifiés et des profils d'habilitation ont été définis pour déterminer les types de données accessibles à une catégorie d'utilisateur.

Selon l'article 32§4 du règlement, le responsable du traitement et le sous-traitant doivent prendre des mesures afin de garantir que toute personne agissant sous leur autorité ayant accès à des données à caractère personnel, ne les traite que sur leur instruction.

Exemple : le gestionnaire de paie accède aux données de paie conformément à ses responsabilités définies dans son profil de poste.

2.9.4 Sécurisation des traces

Le traitement prévoit des dispositifs ou procédures de journalisation centralisée afin de détecter d'éventuels dysfonctionnements et tentatives d'accès illicites aux données.

En effet, l'intégrité et la disponibilité des logs présents sur les équipements peuvent être altérées lors d'une cyber-attaque.

Exemple : en cas de cyber-attaque conduisant à une fuite de données probable, disposer d'un « puit de logs » indépendant du système informatique mis à mal est une source d'analyse pertinente pour identifier les étapes de l'attaque et les possibles fuites de données.

2.9.5 Sécurisation des interconnexions

Toute mise en relation automatisée d'informations provenant de fichiers ou logiciels distincts a été préalablement identifiée. Les données ainsi transportées doivent faire l'objet d'un niveau de sécurité adapté.

La CNIL identifie trois critères cumulatifs permettant de qualifier l'existence d'une interconnexion entre des fichiers[17] :

1. L'objet de l'interconnexion doit être la mise en relation de fichiers ou de traitements de données à caractère personnel ;
2. Cette mise en relation concerne au moins deux fichiers ou traitements de données à caractère personnel distincts ;
3. Il s'agit d'un processus automatisé ayant pour objet de mettre en relation des informations issues de ces fichiers ou de ces traitements.

Par exemple : Le croisement de ces extractions

2.10 Infogérance

Dans le cas de l'infogérance, les risques spécifiques ont été évalués en amont (maîtrise du système d'information (SI), actions à distance, hébergement mutualisé, etc.) afin de prendre en compte, dès la rédaction des exigences applicables au futur prestataire, les besoins et mesures de sécurité adaptés.

[17] https://www.cnil.fr/en/node/15316

Toute entité qui souhaite externaliser son système d'information ou ses données, doit en amont évaluer les risques spécifiques à l'infogérance afin de prendre en compte, dès la rédaction des exigences applicables au futur prestataire, les besoins et mesures de sécurité adaptés.

2.11 Maintenance

Pour garantir que des données ne seront pas compromises lors d'une intervention de maintenance, les risques inhérents sont évalués en amont et des mesures de sécurité techniques et organisationnelles adaptées sont prises par l'organisme.

Dans certains cas, la mise en œuvre d'une liaison permettant d'intervenir à distance est indispensable, notamment en cas de besoin élevé en disponibilité du système d'information (exemple : télédiagnostic d'un progiciel de gestion). L'exploitation de vulnérabilités sur un dispositif de télémaintenance est susceptible de faciliter les intrusions dans le système d'information et d'affecter ainsi la sécurité de l'ensemble du SI.

2.12 Sauvegardes

Des sauvegardes des données sont effectuées à échéance régulière conformément à la Politique de sauvegardes de l'organisme. La politique de sauvegarde a pour objectif de définir des exigences en matière de sauvegarde de l'information, des logiciels et des systèmes. Suite à un incident d'exploitation ou en contexte de gestion d'une intrusion, la disponibilité de sauvegardes conservées en lieu sûr est indispensable à la poursuite de l'activité.

Une sécurisation renforcée est mise en œuvre pour les sauvegardes des données sensibles ou jugées confidentielles par l'organisme. Par exemple, par une mesure de chiffrement ou une traçabilité renforcée des accès et des opérations effectuées sur les sauvegardes.

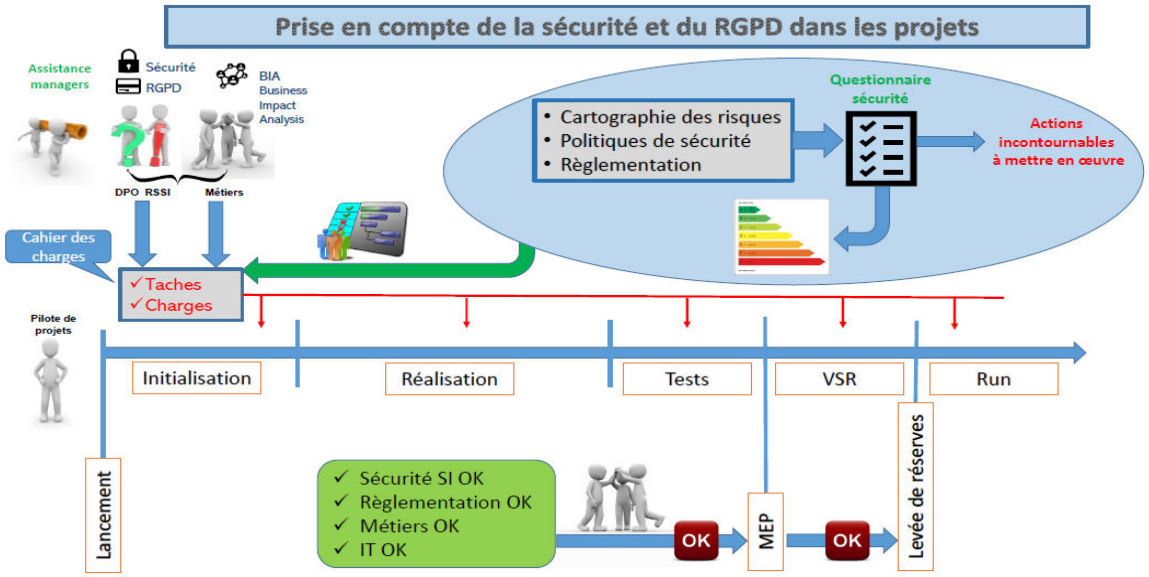
2.13 Violations de données[18]

L'organisation doit disposer de procédures adéquates pour détecter, rapporter et analyser toute violation de données (destruction, perte, altération, divulgation ou accès non autorisé à des données…).

Elle devra également adapter ses processus pour se conformer aux obligations du RGPD.

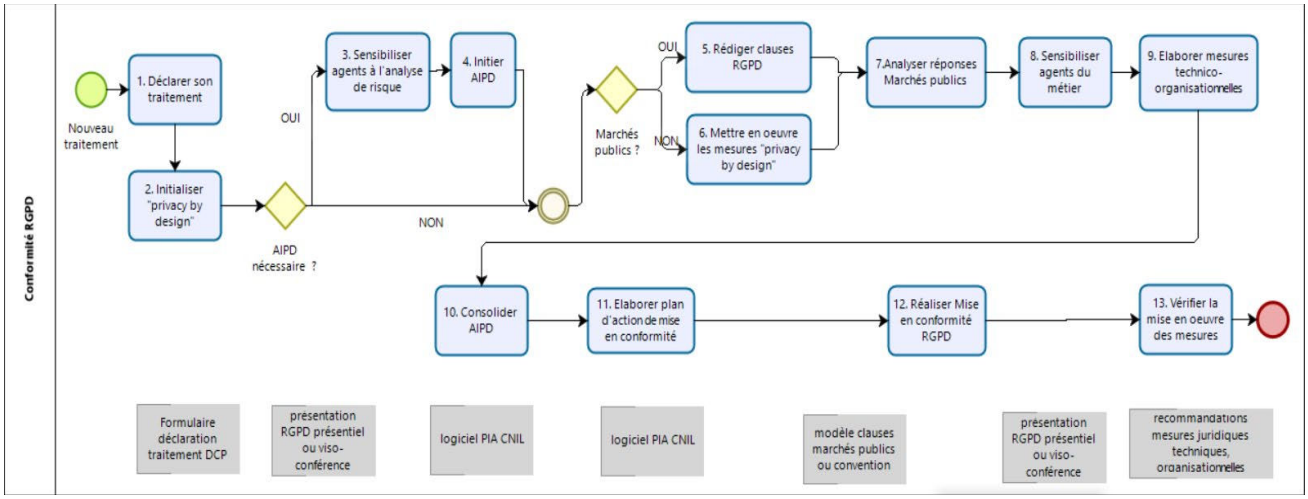
[18] https://clusif.fr/publications/quest-ce-quune-violation-de-donnees-personnelles/

3 Infographies



Source : Maisons & Cités

L'objectif est d'illustrer le processus général d'intégration et d'organisation de la sécurité, du RGPD et dans tous les projets, qu'ils soient automatisés (informatiques) ou manuels (papiers). Il permet de déterminer les actions obligatoires et complémentaires de sécurité et de protection des données, et ce, avant la mise en production du traitement.



Source : Conseil départemental de la Seine Saint-Denis

Ce macro-processus décrit les différentes étapes du processus interne "Privacy by Design" dans le cadre de la conduite d'un projet d'informatisation. Il permet de s'inscrire dans une démarche plus globale de projet et d'acculturer progressivement les acteurs internes (chefs de projet informatique (MOE) et métiers (MOA)) aux différentes étapes nécessaires à la mise en conformité au RGPD.

4 Acteurs

4.1 Le délégué à la protection des données

Le Délégué à la protection des données (DPD ou DPO en anglais)[19] doit être consulté en amont sur toutes les questions relatives à la protection des données personnelles concernant le projet.

Selon l'article 38 du règlement, le responsable du traitement et le sous-traitant doivent veiller à ce que le délégué à la protection des données, lorsqu'il existe, soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Ceci implique notamment la consultation du DPO ou du Chargé de conformité RGPD lors de la conception et du paramétrage de solutions informatiques traitant des données personnelles.

4.2 Le RSSI

Le RSSI (responsable de la sécurité des systèmes d'information) a été consulté en amont sur la sécurité des systèmes et des outils traitant de l'hébergement de données à caractère personnel.

Le RSSI et le DPO doivent collaborer de manière étroite telle que développée dans la fiche consacrée à ce sujet. [20]

4.3 Les Responsable(s) de traitements[21]

Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse prévue par les dispositions législatives ou réglementaires relatives à ce traitement, *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (RGPD, Art. 4.7).*

En pratique, il s'agit de la personne morale incarnée par son représentant légal.

Si le responsable du traitement est juridiquement le représentant légal de l'organisation, il convient d'identifier les acteurs internes ou externes qui contribuent de manière opérationnelle à cette responsabilité dans la mise en œuvre du projet. Les employés traitant les données à caractère personnel au sein de l'organisation agissent pour exécuter les missions confiées par le responsable du traitement[22].

4.4 Les responsables de traitement conjoints

En cas de détermination conjointe des finalités et des moyens du traitement par différents acteurs, les cas de co-responsabilité ont été identifiés et des accords ont été conclus afin de définir de manière transparente la responsabilité et le rôle de chacun.

Selon l'article 26 du RGPD, lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont juridiquement considérés comme les responsables conjoints du traitement. Ceux-ci définissent de manière transparente

[19] https://clusif.fr/publications/faq-rgpd-le-delegue-a-la-protection-des-donnees/

[20] https://clusif.fr/publications/faq-rgpd-synergies-avec-le-rssi/

[21] https://clusif.fr/publications/faq-rgpd-quelles-sont-les-obligations-du-responsable-de-traitement-rt/

[22] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fr

leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement.

Cela inclut les services et les responsables internes, et les structures ou prestataires externes.

4.5 Les sous-traitants

Les relations Responsable de traitements (client) / Sous-traitant (prestataire) mettant en œuvre des traitements de données au sein du projet sont régies par des contrats et/ou actes juridiques définissant clairement les obligations des parties. [23]

En application de l'article 28 du RGPD, la réalisation d'un traitement par un prestataire agissant en tant que sous-traitant selon la définition du règlement, doit être régie par un contrat ou tout autre acte juridique, liant le sous-traitant au responsable du traitement et définissant l'objet et la durée du traitement, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées. Le document doit tenir compte des tâches et responsabilités spécifiques du sous-traitant dans le cadre du traitement à effectuer et du risque pour les droits et libertés de la personne concernée.

4.6 Autres Tiers

L'ensemble des tiers et/ou destinataires susceptibles de recevoir la communication de données à caractère personnel dans le cadre du traitement doivent être identifiés.

Selon les articles 13 et 14 du RGPD, toute personne concernée par un traitement des données a le droit de connaître et de se faire communiquer, en particulier, l'identité des destinataires de ses données à caractère personnel.

Selon l'article 19 du même règlement, 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 du traitement, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires, si celle-ci en fait la demande.

[23] https://clusif.fr/publications/responsabilite-des-sous-traitants/

5 Risques de sanctions

Dans le cadre de ses missions d'audit et de contrôle, l'autorité de contrôle (en France, la Commission Nationale Informatique et Libertés - CNIL), veille à ce que les amendes administratives imposées en vertu de l'article 83 du RGPD soient dans chaque cas, effectives, proportionnées et dissuasives.

Les amendes administratives peuvent aller jusqu'à 10 000 000 voire 20 000 000 euros selon les cas, ou dans le cas d'une entreprise, jusqu'à 2 voire 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives.

Les États membres notifient à la Commission européenne les dispositions légales qu'il adopte en vertu du paragraphe 1 et, sans tarder, toute modification ultérieure les concernant.

D'après l'article 84 du RGPD, les États Membres peuvent également mettre en place des sanctions supplémentaires en cas de violation du RGPD, en fonction de la marge de manœuvre dont ils disposent pour encadrer certains traitements de données. Il s'agit surtout de réprimander les violations qui ne font pas l'objet d'amendes administratives au sens de l'article 83 du RGPD.

Ces sanctions sont mentionnées en France à la section « Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques » (articles 226-16 à 226-24) du code pénal. Il existe ainsi une sanction pénale en cas de détournement de la finalité des données personnelles lors d'un traitement de données (article 226-21 du code pénal).

Les sanctions pénales peuvent aller jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende (article 226-16 du code pénal).

Sources :

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre8#Article83

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre8#Article84

https://www.legalplace.fr/guides/rgpd-sanction/

Beaucoup de sociétés ont fait l'objet de sanctions de la part de la CNIL en raison du non respect des obligations qu'imposent le RGPD[24]. Une des récentes sanctions de la CNIL à l'encontre d'une grande société illustre la nécessité d'avoir une démarche de « *privacy by design* ». Les manquements suivants ont notamment été retenus :

- Durée de conservation des données excessives ;
- Conservation excessive des pièces d'identité lors d'une demande d'exercice des droits (article12.6) ;
- Retard dans le traitement des demandes d'exercice des droits ;
- Mentions d'informations incomplètes (article 13) ou compliquées ;
- Droit à l'effacement insuffisamment respecté (article 21) ;
- Manquement à l'obligation de sécurité (article 32) ;
- Défaut de déclaration de violation de données (article 33) ;
- Manquement à l'obligation de loyauté (article 5.1 a).

[24] https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil

Tour Eria
5 rue Bellini
92821 Puteaux cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr