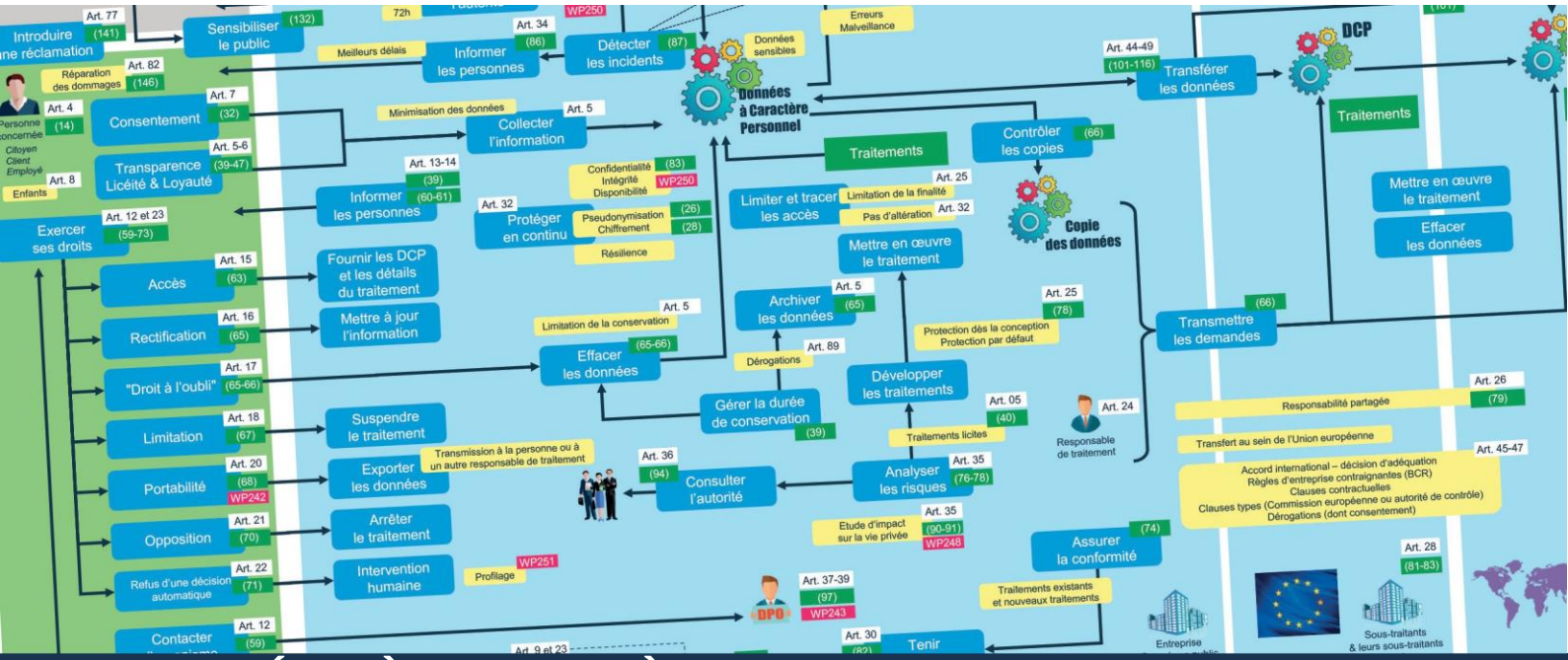
LES FICHES PRATIQUES du CLUSIF - RGPD



DONNÉES À CARACTÈRE PERSONNEL

1. QU'EST-CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL[1] (DCP)

Constitue une donnée personnelle, *toute information se rapportant à une personne physique identifiée ou identifiable*[2] (dénommée *personne concernée*). Une personne physique identifiable peut être identifiée, *directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (RGPD, Art. 4.1)*. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. Le règlement s'applique donc que les données soient directement ou indirectement personnelles.

[1] Dans ce document, les termes « donnée personnelle » et « donnée à caractère personnel » (DCP) sont synonymes. Ils correspondent également à la notion de « personal data » pour la version anglaise du règlement et englobe le « PII : Personally Identifiable Information » utilisé dans le cadre normatif (ISO, NIST) et aux USA (https://www.afnor.org/wp-content/uploads/2017/02/AFNOR_Guide_Protection_des_donnees_perso_HD.pdf).

[2] Dans ce document, les mentions en italique sont des citations des textes législatifs et réglementaires.

La notion de *donnée sensible* n'est explicite que dans les considérants du règlement (*RGPD, C10 et C51* notamment). Le règlement les mentionne sous les termes de *catégories particulières de données à caractère personnel* et de *données relatives aux condamnations pénales et infractions (RGPD, Art.9 et 10)*. Pour autant, la CNIL définit cette notion comme toute *information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.* Le G29 évoque la notion de données à caractère hautement personnel. Il y a parfois confusion entre les données qui sont sensibles pour une organisation et le régime juridique des données sensibles, au sens de la loi française.

Les catégories de données décrites dans le règlement reprennent en les étendant les catégories présentes dans la loi Informatique et Libertés du 6 janvier 1978 modifiée, accordant à celles-ci un niveau de sécurité spécifique.

Le tableau ci-après liste les principales catégories de données à caractère personnel[3].

Types de données	Catégories de données
DCP courantes	État-civil, identité, données d'identification
	Vie personnelle (habitudes de vie, situation familiale, hors données sensibles ou dangereuses…)
	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'événements…)
	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

ⓘ *Du point de vue du RSSI*

Le niveau de sensibilité d'une donnée est différent selon les acteurs de l'organisation. Il peut s'agir de DCP, mais aussi de données comptables ou financières, de données contractuelles, de données liées à l'innovation, de données techniques (mots de passe)…

Ainsi, une donnée peut être sensible (critique) pour l'organisation sans être sensible au titre d'une réglementation. Par exemple, l'adresse d'une personne protégée ou d'une personnalité publique peut être considérée comme sensible.

La difficulté est d'avoir le même vocabulaire au sein de l'organisation, d'identifier et de classifier les données en fonction de l'impact qu'il y a à détenir et traiter cette information. Il est donc important de tenir compte du contexte (cf. analyse de risques / PIA).

Le RSSI doit protéger l'ensemble des données sensibles de l'organisation.

[3] Tableau inspiré du Guide CNIL PIA, Les bases de connaissances, édition février 2018, p.2 : https://www.cnil.fr/fr/PIA-privacy-impact-assessment

2. QU'EST-CE QU'UN TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL ?

Le règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Un traitement de données à caractère personnel est *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction (RGPD, Art. 4.2)*.

La finalité constitue l'objectif principal d'un traitement de données à caractère personnel (gestion des recrutements, gestion des clients et prospects, enquête de satisfaction, surveillance des locaux, profilage, liste d'exclusion, etc.)

Un fichier est un ensemble structuré de données à caractère personnel, accessibles selon des critères déterminés.

- Fichiers de mauvais payeurs
- Contrôle d'accès biométriques
- Vidéosurveillance
- Gestion du personnel et administration des salaires
- Déchiquetage de documents contenant des données à caractère personnel
- Fichiers clients (entreprises)
- Fichiers usagers (administrations)
- Fichiers fournisseurs
- Annuaire interne
- Contrôle d'accès (badgeuses)
- Enregistrement sur l'autocommutateur téléphonique (numéros de téléphone, durée, coût des communications)
- Fichier du restaurant d'entreprise
- Site Internet
- Collecte ou corrélation de logs de serveurs
- IDS/IPS (pour déterminer l'existence d'infractions pénales)
- Envoi d'e-mails promotionnels (voir aussi la directive 2002/58/CE)
- etc.

Figure 1 : exemples de traitement de DCP

ⓘ *Du point de vue du RSSI*

Certains traitements (contrôle de la messagerie, de l'usage d'internet…) prévus pour la protection de l'organisation, peuvent engendrer un risque pour les droits et libertés individuelles des collaborateurs. Il est important de recenser et d'analyser ces traitements induits par la sécurité au même titre que les traitements métiers de l'organisation.

3. PEUT-ON METTRE EN ŒUVRE UN TRAITEMENT AVEC DES DONNÉES SENSIBLES ?

Le règlement interdit par principe le traitement de données à caractère personnel dites sensibles au motif qu'elles méritent une protection spécifique, compte tenu des risques importants pour les droits et libertés fondamentaux inhérents à leur traitement (*RGPD, Art. 9 et 10*).

Il y a toutefois des exceptions, déjà présentes dans la loi Informatique et Libertés de 1978 mais le règlement étend ou limite parfois leur champ d'application (*RGPD, Art. 9*). Le nouvel article 8 de la loi Informatique et Libertés (LIL) précise l'interdiction de principe de collecter ce type de données et les exceptions.

RGPD	LIL
Consentement de la personne *consentement explicite*	*consentement exprès*
Traitement nécessaire à l'exécution des droits et obligations du responsable du traitement en matière de droit du travail et droit de la sécurité sociale	**-**
Sauvegarde des intérêts vitaux *personne concernée ou autre personne physique dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement*	**Sauvegarde de la vie humaine** *la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle*
Associations et assimilées *fondation, association ou tout autre organisme à but non lucratif poursuivant une finalité politique, philosophique, religieuse ou syndicale*, pour l'objet de ladite association, et dans la mesure où le traitement ne concerne que les membres de l'association et que les données ne sont pas communiquées à des tiers	*association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical*
Données rendues publiques par la personne *données à caractère personnel qui sont manifestement rendues publiques par la personne concernée*	*données à caractère personnel rendues publiques par la personne concernée*
Constatation, exercice ou défense d'un droit en justice	(idem)
Intérêt public *motif d'intérêt public important qui doit être proportionné à l'objectif poursuivi*	*justifié par l'intérêt public et autorisé dans les conditions de l'article 26* [sûreté, défense, sécurité publique…]
Santé *médecine préventive, médecine du travail, appréciation de la capacité de travail du travailleur, diagnostics médicaux, prise en charge sanitaire et sociale, gestion des systèmes et des services de soins de santé ou de protection sociale*	*médecine préventive, diagnostics médicaux, administration de soins ou de traitements, gestion de services de santé,* mis en œuvre par un professionnel de santé ou une personne soumise au secret professionnel
Traitements nécessaires pour des motifs d'intérêt public dans le domaine de la santé publique protection contre les menaces transfrontalières graves pesant sur la santé, ou pour garantir des normes élevées de qualité et de sécurité des soins et des médicaments	**-**
Archivage dans l'intérêt public ou à des fins historiques, statistiques ou scientifiques	**-**
-	**Traitements statistiques de l'INSEE**

-	**Données de santé** *Traitements comportant des données concernant la santé justifiés par l'intérêt public et conformes aux dispositions du chapitre IX de la loi de 1978 [recherche, étude, évaluation dans le domaine de la santé]*
-	**Données biométriques nécessaires au contrôle d'accès aux lieux de travail** Traitements mis en œuvre par l'employeur ou les administrations et portant sur les données biométriques nécessaires au contrôle d'accès aux lieux de travail et nécessaires aux missions confiées aux salariés, agents ou prestataires {nouveauté}
-	**Informations publiques figurant dans les jugements et décisions de justice** Traitements portant sur la réutilisation des informations publiques figurant dans les jugements et décisions de justice sous réserve de ne pouvoir réidentifier les personnes {nouveauté}
-	**Traitements nécessaires à la recherche publique** au sens de l'article L.112-1 du code de la recherche.

Tableau 2 : Exceptions à l'interdiction de traitements de données "sensibles"

Le traitement doit être en tout état de cause proportionné au but poursuivi, respecter les droits des personnes concernées et prévoir des mesures appropriées et spécifiques en vue de sauvegarder les droits fondamentaux et les intérêts légitimes de la personne concernée.

Voir aussi « Les principes du règlement » dans la FAQ.

4. QUI EST RESPONSABLE DE TRAITEMENT ?

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.

Les employés traitant les données à caractère personnel au sein de l'organisation agissent pour exécuter les missions confiées par le responsable du traitement[4].

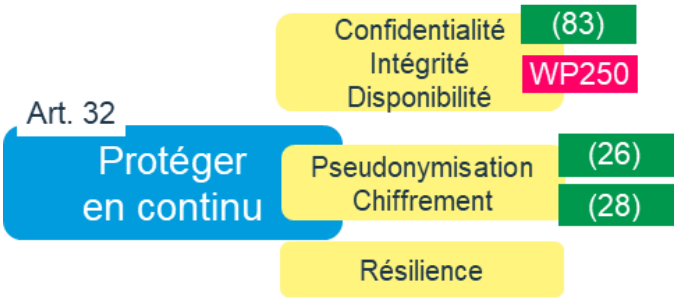
Il y a responsabilité conjointe du traitement si plusieurs organisations s'associent pour déterminer « pourquoi » et « comment » les données à caractère personnel devraient être traitées. Les responsabilités respectives au regard du règlement seront formalisées dans un accord entre les différentes organisations.

La norme ISO/IEC 29100:2011 traite des concepts de PII Principals, PII Controller et PII Processor[5].

[4] 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

[5] https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:29100:ed-1:v1:en

5. QUELLES MESURES TECHNIQUES PEUT-ON METTRE EN PLACE POUR PROTÉGER LES DONNÉES ?



Il faut noter qu'une donnée anonymisée n'est tout simplement plus soumise au règlement puisqu'elle ne contient par définition pas de données à caractère personnel. Mais l'anonymisation véritable est très difficile car il s'avère dans les faits presque toujours possible de réidentifier la personne concernée en croisant des informations ou par connaissance du domaine.

Parmi les mesures techniques, le règlement mentionne explicitement le chiffrement et la pseudonymisation comme des mesures concrètes permettant de réduire les risques.

Le chiffrement n'est pas une forme d'anonymisation, mais une mesure de protection. La chaîne de caractères « Mickey Mouse » peut ainsi devenir « 1#e$*fgo8foep*#5 » en y appliquant un algorithme utilisant une clé de chiffrement. Il y a alors deux approches possibles :

- Avec du chiffrement symétrique, la même clé permet de faire marche arrière et de retrouver « Mickey Mouse ». Il faut donc faire attention à ne pas perdre cette clé si l'on souhaite protéger ses données…

- Avec du chiffrement asymétrique, c'est une autre clé qui réalise l'opération inverse pour rendre les données à nouveau visibles. Cela revient en pratique à disposer d'une clé pour fermer une porte d'entrée et une autre pour l'ouvrir. Une copie de la clé de fermeture est donnée (elle est qualifiée de clé publique) à tous ceux qui la demandent. Mais la clé d'ouverture (dite clé privée) n'est conservée que par une personne. On applique le même principe pour le chiffrement des données : la clé publique est diffusée largement et permet à tout le monde de chiffrer de l'information que vous serez le seul à pouvoir déchiffrer avec votre clé privée une fois que l'information vous aura été transmise. Entre temps, l'information pourra circuler par exemple sur Internet puisqu'elle sera illisible.

Il existe en théorie une troisième stratégie qui consiste à casser le chiffrement pour décrypter l'information sans aucune clé. Mais les algorithmes modernes sont robustes et leur bonne utilisation vous protège raisonnablement de ce risque. L'ANSSI[6] et la CNIL[7] ont publié des guides détaillés sur le sujet du chiffrement. Le règlement mentionne que la fuite de données chiffrées n'impose pas la communication à la personne concernée, tant que les données restent illisibles, c'est-à-dire tant que les clés n'ont pas été volées (*RGPD, Art. 34.3a*).

La pseudonymisation est définie dans le règlement comme le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise, sans avoir recours à des informations supplémentaires (à condition qu'elles soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne identifiée ou identifiable) (*RGPD, Art. 4*). Elle consiste donc à supprimer des dimensions identifiantes.

[6] https://www.ssi.gouv.fr/particulier/bonnes-pratiques/crypto-le-webdoc/cryptologie-art-ou-science-du-secret/
[7] https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires

Exemple d'un numéro de carte bancaire : « 4312 4535 1342 4987 ».

La technique la plus simple consiste à cacher une partie de l'information, comme dans les relevés de transactions bancaires en ligne, « 4312 4535 XXXX XXXX ».

Il est également possible de masquer le numéro en remplaçant tous les chiffres : « 1234 5764 8394 4040 ». C'est une action irréversible (qui n'a donc rien à voir avec du chiffrement). Sa portée peut être temporaire (masquage en mémoire) ou définitive (masquage dans une base de données).

Les entreprises utilisent parfois aussi la tokenisation, qui consiste à masquer une donnée avant de la partager avec un tiers, mais en gardant une trace de sa valeur initiale dans une table de correspondance, de telle sorte qu'on pourra réidentifier cette valeur en lui redonnant sa vraie valeur quand elle reviendra dans l'entreprise initiale. Si l'on peut estimer que cette technique ressemble à du chiffrement, la différence réside dans le fait que vous ne souhaitez pas partager la vraie information avec ce tiers.

On peut enfin mentionner le hachage : un algorithme permet de calculer une empreinte (le hash) à partir d'un document, d'une image, d'une autre chaîne de caractère… Et cet algorithme garantit (dans une certaine mesure) que cette empreinte sera unique. Dans le cas des mots de passe, plutôt que de les stocker dans une base de données, on peut ainsi appliquer un algorithme de hachage qui calcule donc une nouvelle chaîne de caractère unique, mais qui protège le mot de passe, puisqu'on ne le stocke plus. Quand l'utilisateur saisit son mot de passe, on applique le même algorithme pour vérifier que les deux empreintes correspondent. Dans les faits, d'autres techniques peuvent compléter ce type de mesure pour se protéger des attaques (par salage de l'information notamment).

Le document *WP216 Techniques d'anonymisation*[8] du G29 donne plus de détails sur les techniques d'anonymisation.

ⓘ *Du point de vue du RSSI*

Des mesures techniques sont déjà en place dans l'entreprise. Il s'agira dans un premier temps de les recenser et de vérifier si elles couvrent suffisamment les données à caractère personnel. La généralisation du chiffrement de l'information est aussi une option possible, en accordant une importance particulière à la gestion du cycle de vie des clés de chiffrement.

C'est aussi l'occasion de repenser les stratégies de gestion des jeux de données hors production.

[8] http://www.dataprotection.ro/servlet/ViewDocument?id=1085