9

LES CAHIERS JURIDIQUES
DE LA CHAMBRE DES MÉTIERS

PROTECTION DES DONNÉES PERSONNELLES (RGPD)

CHAMBRE DES MÉTIERS
SERVICES AUX ENTREPRISES

LES CAHIERS JURIDIQUES
DE LA CHAMBRE DES MÉTIERS

PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Fiche 1

RGPD

CHAMBRE DES MÉTIERS
SERVICES AUX ENTREPRISES

Fiche 01 - RGPD

Mise à jour : XX.XX.2024

Le règlement général sur la protection des données (RGPD) établi à partir du 25 mai 2018 un nouveau cadre normatif applicable dans tous les Etats Membres de l'Union Européenne.

Si les grands principes applicables en matière de protection des données personnelles ne sont pas modifiés avec le RGPD, la nouveauté est que les entreprises doivent avoir une approche dynamique et proactive pour anticiper et réduire les risques en la matière.

1. Qu'est-ce que le règlement général sur la protection des données (RGPD) ?

Le RGPD est l'acronyme de Règlement Général sur la Protection des Données, qui est l'appellation simplifiée officielle pour 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, et abrogeant la directive 95/46/CE.* »

Lien vers le RGPD (infobox)

· **Une application directe dans tous les Etats Membres à partir du 25 mai 2018**

L'application directe du RGPD impose au Luxembourg d'abroger la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Un projet de loi prévoit cette abrogation et précise que toute référence à la loi de 2002 sera remplacée par une référence au RGPD et à la présente loi.

Lien vers le projet de loi N°7194 portant création de la CNPD (infobox)

· **La possibilité aux Etats Membres de définir des règles plus spécifiques dans certains domaines**

Le RGPD autorise les Etats Membres à maintenir ou à introduire des dispositions nationales plus spécifiques pour les domaines suivants :

- les traitements nécessaires au respect d'une obligation légale ;
- les traitements nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ;
- les conditions applicables au consentement des enfants ;
- certaines situations particulières de traitements.

En conséquence, le projet de loi N°7194 prévoit des dispositions particulières pour les traitements suivants :

- le traitement aux fins de journalisme ou d'expression universitaire, artistique ou littéraire,
- le traitement aux fins de recherche scientifique ou historique ou à des fins statistiques, et
- le traitement de catégories particulières de données concernant les services de la santé.

Lien vers le projet de loi N°7194 portant création de la CNPD (infobox)

Les traitements des données à caractère personnel des employés dans le cadre de leur travail n'ayant pas fait à ce jour l'objet de dispositions particulières nouvelles, les articles L.261-1 et 2 du code du travail restent d'application.

Lien vers la page « Mon Entreprise -> Droit du travail »

LES CAHIERS JURIDIQUES
DE LA CHAMBRE DES MÉTIERS

PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Fiche 2

DONNÉES À CARACTÈRE PERSONNEL

CHAMBRE DES MÉTIERS
SERVICES AUX ENTREPRISES

Fiche 02 - Données à caractère personnel

Mise à jour : XX.XX.2024

1. Qu’est-ce qu’un traitement de données à caractère personnel ?

· **La notion de donnée à caractère personnel**

Une donnée à caractère personnel est toute information se rapportant à une personne physique identifiée ou identifiable.

Est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

· **La notion de traitement**

Un traitement 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.

LES CAHIERS JURIDIQUES
DE LA CHAMBRE DES MÉTIERS

PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Fiche 3

PANORAMA DES PRINCIPES DE BASE

CHAMBRE DES MÉTIERS
SERVICES AUX ENTREPRISES

Fiche 03 - Panorama des principes de base

Mise à jour : XX.XX.2024

1. Quels sont les principes à respecter ?

I- Les données personnelles doivent être collectées de façon licite, loyale et transparente

· **Concernant la licéité**

Pour pouvoir traiter une donnée personnelle, il faut que la finalité du traitement entre dans au moins une des 6 hypothèses de licéité qui sont prévues.

Le RGPD liste 6 hypothèses dans lesquelles les traitements sont admis.

I- La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques

· **Il faut une déclaration ou un acte positif clair de la personne concernée**

Le consentement est « *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.* »

· **Le consentement doit être donné librement (article 7 (4) du RGPD)**

Suivant le considérant 42 du RGPD le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice.

Cette condition rend peu probable que le consentement puisse servir de base aux traitements de données au travail sauf si l'employé peut refuser sans que ce refus n'est de conséquence négative.

· **La personne concernée a le droit de retirer son consentement à tout moment (article 7 (3) RGPD)**

En cas de retrait du consentement le responsable du traitement risque aussi de devoir effacer les données (article 17 du RGPD).

II-Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie

III- Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis

IV- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique

V- Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement

· **La balance des intérêts**

La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur cette hypothèse (article 21 (1) du RGPD).

Dans ce cas, c'est au responsable du traitement de démontrer qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée pour continuer le traitement.

VI- Le traitement est nécessaire aux fins de l'intérêt légitime du responsable du traitement à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée

· **La balance des intérêts**

La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur cette hypothèse (article 21 (1) du RGPD).

En cas d'opposition de la personne concernée, c'est au responsable du traitement de démontrer qu'il existe des motifs légitimes et impérieux qui prévalent sur les intérêts et les droits et libertés de la personne concernée pour continuer le traitement.

· **Exemples d'intérêts légitimes**

Suivant le considérant 47 du RGPD, un intérêt légitime pourrait, par exemple, exister :

- lorsque la personne concernée est un client du responsable du traitement ou est à son service ;
- pour un traitement de données à caractère personnel à des fins de prospection.

· **Concernant la loyauté et la transparence**

Le responsable du traitement doit informer la personne concernée qu'il traite ses données, et aussi comment il traite les données en communiquant notamment la finalité et la base juridique du traitement.

Cf Articles 13 et 14 du RGPD. Lien vers le RGDP (infobox)

Le principe de transparence exige que toute information et toute communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples.

II- Les données personnelles doivent être collectés pour une finalité bien déterminée

Suivant ce principe, il est exigé que les données soient collectées pour des finalités déterminées, explicites, et légitimes.

Ce principe impose aussi que les données ne soient pas traitées ultérieurement de manière incompatible avec ces finalités.

Le RGPD fixe une série de critères permettant de déterminer la compatibilité d'un traitement ultérieur dont les suivants (art.6(4) du RGPD) :

- l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;
- le contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement.

Il est possible de traiter des données à une fin différente sans s'interroger sur la compatibilité dans deux cas :

- si la personne concernée a donné son consentement ;
- si le traitement ultérieur est légalement prévu.

On notera que les traitements ultérieurs à des fins archivistiques dans l'intérêt public, à des fins

de recherches scientifique ou historique, ou à des fins statistiques sont considérés comme compatibles sous certaines conditions (article 89 (1) du RGPD).

III- Seules les données nécessaires doivent être collectées

Seules les données adéquates, pertinentes et nécessaires doivent être collectées (le principe de la minimisation des données).

IV- Une durée de conservation proportionnée doit être déterminée

La durée de conservation des données doit être limitée au strict minimum.

Afin de garantir que les données ne soient pas conservées au-delà du nécessaire il est conseillé de fixer des délais pour l'effacement des données, ou pour une vérification périodique (considérant 39 du RGPD).

V- Les données doivent être exactes

Les données doivent être mises à jour, et toute inexactitude doit être corrigée sans tarder.

VI- Il faut assurer l'intégrité et la confidentialité des données

Il s'agit de l'obligation d'assurer la sécurité de données auquel s'ajoute l'obligation de notifier à l'autorité de contrôle, voire aux personnes concernées, les violations de données.

VII- Il faut pouvoir démontrer sa conformité

· La notion d'« accountability »

Le responsable du traitement, non seulement est responsable en cas d'une violation au RGPD, mais aussi qu'il doit être à même de démontrer que ses traitements sont en conformité avec les différents principes.

· L'obligation de cartographier les traitements

L'article 30 du RGPD impose l'obligation pour les responsables de tenir un « registre des activités de traitements » mais une exception est prévue pour les entreprises de moins de 250 employées sauf si :

- le traitement n'est pas occasionnel ;
- le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées ;
- le traitement porte notamment sur une donnée sensible.

Des modèles de registres sont proposées par les autorités nationales de contrôle, comme par exemple :

- le «Compliance Support Tool » de la CNPD (Lux)

https://cnpd.public.lu

- le registre proposé par la CNIL (Fr.)

https://www.cnil.fr/

LES CAHIERS JURIDIQUES
DE LA CHAMBRE DES MÉTIERS

PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Fiche 4

AIPD

CHAMBRE DES MÉTIERS
SERVICES AUX ENTREPRISES

Fiche 04 - AIPD

Mise à jour : XX.XX.2024

- **L’analyse d’impact (article 35 du RGPD)**

L’analyse d’impact doit définir les risques encourus pour les droits et libertés des personnes concernées, et les solutions pour y faire face.

Une analyse d’impact est notamment imposée en cas d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques fondée sur un traitement automatisé (y compris le profilage) et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique.

LES CAHIERS JURIDIQUES
DE LA CHAMBRE DES MÉTIERS

PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Fiche 5

LA SOUS TRAITANCE RGPD

CHAMBRE DES MÉTIERS
SERVICES AUX ENTREPRISES

Fiche 05 - La sous traitance RGPD

Mise à jour : XX.XX.2024

1. Les obligations particulières en cas de sous-traitance

Les obligations particulières portent sur :

- Le choix du sous-traitant qui doit présenter des garanties suffisantes
- Le traitement de données personnelles par un sous-traitant doit être encadré par un contrat qui doit comprendre certaines mentions listées à l'article 28 du RGPD
- Le sous-traitant doit tenir un registre des traitements qu'il effectue pour le compte d'un responsable

LES CAHIERS JURIDIQUES
DE LA CHAMBRE DES MÉTIERS

PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Fiche 6

DONNÉES SENSIBLES

CHAMBRE DES MÉTIERS
SERVICES AUX ENTREPRISES

Fiche 06 - Données sensibles

Mise à jour : XX.XX.2024

1. Le traitement des données sensibles

· **La liste des données sensibles a été étendue par les données génétiques et biométriques.**

Suivant l'article 9 du RGPD, cette liste comprend :

- les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale,
- les données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle
- les données génétiques et les données biométriques aux fins d'identifier une personne physique de manière unique.

· **L'importance du contexte du traitement**

En présence de données qui ne sont pas dans tous les cas considérées comme sensibles, comme une photographie, le RGPD propose de prendre en compte le contexte pour déterminer s'il s'agit d'un traitement d'une donnée sensible.

Suivant le considérant 51, il ne faut pas faire systématiquement entrer toute photographie dans la définition d'une donnée sensible, mais seulement si les photographies « *sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique*.»

Une photographie sur un badge pour accéder à un local devrait être considérée comme une donnée sensible.

· **Le principe de l'interdiction du traitement d'une donnée sensible**

Le principe de l'interdiction est assorti de nombreuses exceptions.

Il convient de se référer à l'article 9 (2) du RGPD. Lien vers le RGPD (infobox)