LES DONNÉES PERSONNELLES

ET LE RÈGLEMENT DE 2016

QU'ES-CE QU'UNE DONNÉE ?

HISTORIQUE DE LA RÈGLEMENTATION

LA RÈGLE POUR 2018

QUI DOIT SE CONFORMER ?

COMMENT SE CONFORMER ?

QU'ES-CE QU'UNE DONNÉE ?

"Représentation conventionnelle d'une information en vue de son traitement informatique."

Dictionnaire Larousse

Les données sont des traductions froides et objectives d'informations recueillies sur un usager ou par extension sur ses biens (matériel informatique, etc.). Il en existe plusieurs types, plus ou moins protégées.

DONNÉES NON PERSONNELLES

DONNÉES PERSONNELLES

DONNÉES NON PERSONNELLES

Toutes les données ne revêtent pas un caractère personnel. Certaines ne permettent pas l'identification d'une personne ou d'un groupe de personnes. La protection à laquelle les données non personnelles sont soumises est donc plus souple. Cependant il faut rester vigilant car le croisement de données non personnelles peuvent parfois permettre l'identification d'un individu.

DONNÉES PERSONNELLES

Une donnée est dite personnelle lorsqu'elle porte sur une personne en particulier et non plus sur des éléments généraux.

"Toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant [nom, numéro d'identification, localisation, etc.] ou à un ou plusieurs éléments spécifiques propres à son identité [...]."
Règlement 2016/679, Article 4

DONNÉES SENSIBLES

DONNÉES DES MINEURS

DONNÉES SENSIBLES

"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." (Glossaire CNIL)

L'article 9 définit les 10 cas dans lesquels la collecte des données sensibles est possible.

1) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques.

2) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale.

3) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.

4) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale.

5) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée.

6) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

7) le traitement est nécessaire pour des motifs d'intérêt public important.

8) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale. Le traitement doit alors être réalisé par une personne soumise au secret médical.

9) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique.

10) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

DONNÉES DES MINEURS

On parle de données de mineur lorsqu'on est en présence de mineurs de 16 ans, au delà les règles sont les mêmes que pour les adultes. Ces mineurs étant considérés comme plus fragiles que les majeurs, la collecte des données qui les concernent ne peut se faire sans l'accord des parents.
Chaque Etat membre a la possibilité d'abaisser l'âge en question jusqu'à 13 ans au lieu de 16.

LES DONNÉES PERSONNELLES

ET LE RÈGLEMENT DE 2016

QU'ES-CE QU'UNE DONNÉE ?

HISTORIQUE DE LA RÈGLEMENTATION

LA RÈGLE POUR 2018

QUI DOIT SE CONFORMER ?

COMMENT SE CONFORMER ?

HISTORIQUE DE LA RÈGLEMENTATION

- 1978 : la France adopte la loi "Informatique et libertés"
- 1995 : Directive européenne 95/46 "protection des données personnelles"
- 2004 : refonte de la loi "Informatique et Libertés" de 1978
- 2010 : reconnaissance du droit à la protection des données personnelles comme un droit fondamental de l'UE (Art. 8 de la Charte européenne des droits fondamentaux)
- 2016 (14 avril) : adoption du nouveau règlement européen relatif à la protection des données
- 2018 (25 mai) : entrée en vigueur du règlement de 2016

LES DONNÉES PERSONNELLES

ET LE RÈGLEMENT DE 2016

QU'ES-CE QU'UNE DONNÉE ?

HISTORIQUE DE LA RÈGLEMENTATION

LA RÈGLE POUR 2018

QUI DOIT SE CONFORMER ?

COMMENT SE CONFORMER ?

LA RÈGLE POUR 2018

Le règlement de l'Union Européenne 2016/679 vient modifier la réglementation applicable en matière de données personnelles. Ces modifications entreront en vigueur en mai 2018.

COLLECTE DES DONNÉES

EXPLOITATION DU FICHIER

RÉGIMES PARTICULIERS

DROITS DES PERSONNES

COLLECTE DES DONNÉES

LES PRINCIPES

PRIVACY BY DESIGN

LES PRINCIPES

En matière de données, on retrouve six grandes lignes qui doivent guider l'action des responsables de traitement lors de leur collecte. L'Article 5 nous dit que les données doivent être :

Licéité, loyauté, transparence

"a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);"

Limitation des finalités

"b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);"

Minimisation des données

"c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);"

Exactitude

"d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);"

Limitation de la conservation

e) 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; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

Intégrité et confidentialité

"f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);"

PRIVACY BY DESIGN

En français, « protection des données dès la conception ». Ce principe introduit par le règlement impose que les entités à l'origine de la collecte des données doivent prendre en compte les exigences relatives à la protection des données personnelles dès la conception des produits, services et systèmes exploitant des données à caractère personnel.

Article 25 :
Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.
Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.
Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article.

EXPLOITATION DU FICHIER

Une fois collectées, les données font l'objet d'un traitement. Par ce terme, le règlement européen entend l'ensemble des actions qui vont être effectuées sur les données : de la collecte à la destruction en passant par la modification, l'organisation ou la transmission.

Ce traitement doit répondre à deux principales exigences à savoir qu'il doit être licite mais aussi garantir la sécurité des données traitées.

Pour être licite, le traitement doit être justifié ou consenti librement par la personne. Concernant la sécurité, elle peut être optimisée via la pseudonymisation ou le chiffrement par exemple.

LA LICÉITÉ

LA SÉCURITÉ

LA LICÉITÉ

Article 6 :

1) Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

e) 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;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

LA SÉCURITÉ

Article 32 :
1) Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) 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;

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

RÉGIMES PARTICULIERS

Certains cas particulièrement délicats ou sensibles font l'objet d'une règlementation spécifique. Compte tenu de la grande variété des cas, il est impossible de tous les aborder ici mais voici les plus courants :

Les mineurs

Le cas des mineurs de moins de 16 ans implique nécessairment le consentement des parents (ou du responsable légal) à la collecte. En l'absence de ce consentement, le traitement serait alors illicite et le responsable s'exposerait à des sanctions.

Les données sensibles

Les données sensibles font l'objet d'une protection renforcée. Leur collecte doit procéder d'un consentement explicit sauf raisons d'intérêt général ou dans l'intérêt particulier de la personne visée. L'article 9 du règlement prévoit l'ensemble des cas où la collecte des données sensibles est licite.

Données médicales

Les données médiacles sont une catégorie des données sensibles. La collecte de ces données est strictement encadrée du fait de leur grande confidentialité et de leur caractère intime. La personne qui les collecte doit être un professionnel de la santé soumis au secret professionnel. Article 9-3

DROITS DES PERSONNES

- DROIT D'INFORMATION
- DROIT D'ACCÈS
- DROIT DE RECTIFICATION
- DROIT D'OPPOSITION
- DROIT À L'EFFACEMENT
- DROIT À LA PORTABILITÉ
- ACTIONS COLLECTIVES
- EN CAS DE VIOLATION

DROIT D'INFORMATION

Lorsque les données d'une personne sont collectées, le responsable est dans l'obligation de fournir à cette personne un certain nombre d'informations telles que son identité, la finalité de la collecte, les destinataires éventuels des données, etc.

En savoir plus : Article 13

DROIT D'ACCÈS

La personne dont les données ont été collectées peut demander à ce que le responsable du traitement lui dise si ses données sont ou non traitées, et si c'est le cas elle peut demander à accèder à ses données.

En savoir plus : Article 15

DROIT DE RECTIFICATION

Article 16 : La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.

DROIT D'OPPOSITION

La personne concernée peut s'opposer, à tout moment, à ce que ses données soient traitées, le responsable du traitement devra alors cesser de traiter les données personnelles concernée.

En savoir plus : Article 21

DROIT À L'EFFACEMENT

La personne dont les données sont collectées peut demander la disparition de celles-ci et ainsi voir l'effacement des données la concernant. Alors le responsable du traitement est dans l'obligation d'effacer lesdites données, selon les cas de figure.

En savoir plus : Article 17

DROIT À LA PORTABILITÉ

Il s'agit du droit pour une personne concernée à recevoir ses données sous un format lisible par d'autres responsables de traitement avec pour finalité d'en faire profiter d'autres responsables de traitement. Exemple : un utilisateur de Spotify passe chez Deezer mais souhaite disposer des mêmes suggestions d'écoute.
En savoir plus : Article 20

ACTIONS COLLECTIVES

Article 80 :

1) La personne concernée a le droit de mandater un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel les concernant, pour qu'il introduise une réclamation en son nom, exerce en son nom les droits visés aux articles 77, 78 et 79 et exerce en son nom le droit d'obtenir réparation visé à l'article 82 lorsque le droit d'un État membre le prévoit.

2) Les États membres peuvent prévoir que tout organisme, organisation ou association visé au paragraphe 1 du présent article, indépendamment de tout mandat confié par une personne concernée, a, dans l'État membre en question, le droit d'introduire une réclamation auprès de l'autorité de contrôle qui est compétente en vertu de l'article 77, et d'exercer les droits visés aux articles 78 et 79 s'il considère que les droits d'une personne concernée prévus dans le présent règlement ont été violés du fait du traitement.

EN CAS DE VIOLATION

Article 34 : Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais. [...]

LES DONNÉES PERSONNELLES

ET LE RÈGLEMENT DE 2016

QU'ES-CE QU'UNE DONNÉE ?

HISTORIQUE DE LA RÈGLEMENTATION

LA RÈGLE POUR 2018

QUI DOIT SE CONFORMER ?

COMMENT SE CONFORMER ?

QUI DOIT SE CONFORMER ?

Tout organisme réalisant un traitement de données à caractère personnel (Article 2)

Qu'il s'agisse du responsable direct ou d'un sous-traitant :

Article 3 : Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.

Le règlement s'applique aussi bien aux personnes privées (entreprises, etc) qu'aux personnes publiques (administration, collectivités territoriales, etc) : Article 37.1

Il est nécessaire de désigner un responsable du traitement des données qui peut aussi être un sous traitant :

Article 27 : [...]
3) Le représentant est établi dans un des États membres dans lesquels se trouvent les personnes physiques dont les données à caractère personnel font l'objet d'un traitement lié à l'offre de biens ou de services, ou dont le comportement fait l'objet d'un suivi.
4) Le représentant est mandaté par le responsable du traitement ou le sous-traitant pour être la personne à qui, notamment, les autorités de contrôle et les personnes concernées doivent s'adresser, en plus ou à la place du responsable du traitement ou du sous-traitant, pour toutes les questions relatives au traitement, aux fins d'assurer le respect du présent règlement.
5) La désignation d'un représentant par le responsable du traitement ou le sous-traitant est sans préjudice d'actions en justice qui pourraient être intentées contre le responsable du traitement ou le sous-traitant lui-même.

Le régime et les obligations du sous-traitant sont définis à l'Article 28 : Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

Territoire :

Article 3.2 :
"Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :
a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou

b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union."

LES DONNÉES PERSONNELLES

ET LE RÈGLEMENT DE 2016

QU'ES-CE QU'UNE DONNÉE ?

HISTORIQUE DE LA RÈGLEMENTATION

LA RÈGLE POUR 2018

QUI DOIT SE CONFORMER ?

COMMENT SE CONFORMER ?