RGPD (GDPR):
General Data Protection Regulation

De quoi s'agit-il ?

Le 25 mai 2018, le règlement communautaire sur la protection des données personnelles de l'Union européenne (appelé encore « RGPD » ou « GDPR : General Data Protection Regulation » ou « DSGVO : Datenschutz-Grundverordnung ») entre en vigueur.

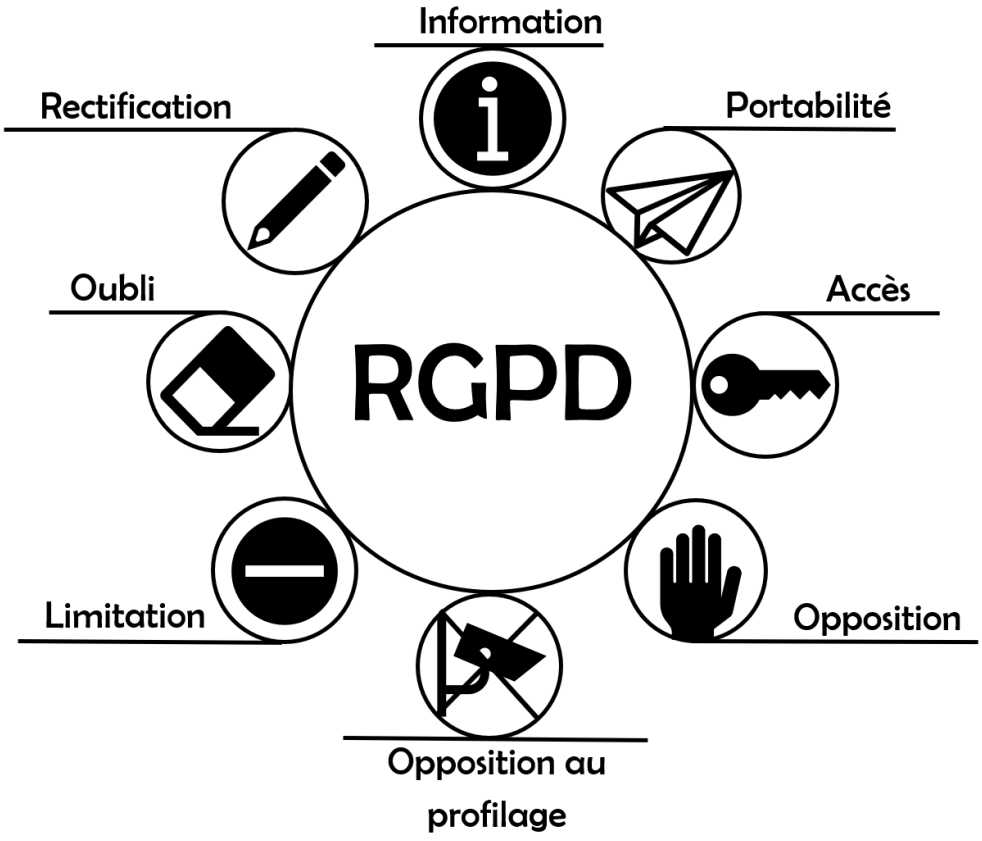
Qu'est-ce qu'un règlement communataire ?

Un règlement communautaire est une sorte de loi dictée par l'Union européenne et qui doit être respectée par tous les États membres, dont le Luxembourg.

En quoi ce règlement me concerne-t-il ?

Vous êtes-vous déjà demandé pourquoi vous recevez toujours les mêmes publicités ou comment une entreprise a pu vous contacter sur votre numéro de téléphone privé ?

En passant des commandes en ligne, en cliquant sur des boutons « J'aime » ou encore en acceptant des cartes de fidélité, nous laissons partout des traces qui permettent de nous identifier. C'est ce que l'on appelle des données personnelles qu'il faudrait protéger.



Le règlement, que vient-il changer et pourquoi était-il nécessaire ?

Il ne faut surtout pas croire que ce règlement est le premier texte en matière de protection des données personnelles. En effet, chaque pays avait déjà sa propre loi qui reprenait les principaux éléments d'une directive européenne de 1995. Au Luxembourg, c'est une loi de 2002 qui régissait la collecte de données et qui sera abrogée le 25 mai 2018.

Jusqu'ici, en matière de données, différentes règles s'appliquaient en fonction du pays où l'on se trouvait. Ceci tentait parfois certaines entreprises à s'installer dans le pays qui leur offrait, selon eux, la « meilleure » loi (ce que l'on appelle « forum shopping »).

De plus, les lois des différents pays n'étaient plus contemporaines et ne prenaient pas forcément en compte les nouvelles technologies et développements dans le domaine informatique.

Enfin dans la plupart des pays, les sanctions n'étaient pas assez élevées de sorte que les lois n'étaient guère respectées, surtout par des entreprises multinationales très peu impressionnées par des sanctions d'environ 150.000 euros.

Le nouveau règlement vient changer cela en augmentant considérablement ce montant. De manière générale, il vise à imposer une même loi dans tous les pays de l'Union Européenne et à améliorer le niveau de protection de nos données personnelles. Concrètement le responsable de traitement, c'est-à-dire celui qui collecte et utilise nos données (une entreprise, une association, une administration…), a plus de devoirs. De l'autre côté, les personnes concernées ont plus de droits.

Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est toute information relative à une **personne physique identifiée ou identifiable**. Une personne est identifiable lorsqu'une information permet de savoir qui elle est directement ou indirectement.

Il peut notamment s'agir de :

- l'adresse postale/électronique
- la date d'anniversaire
- l'empreinte génétique
- le numéro de téléphone
- le numéro de carte bancaire
- le numéro de sécurité sociale
- le numéro étudiant
- l'adresse IP de l'ordinateur
- l'image (photos et vidéos) d'une personne physique
- la donnée de géolocalisation : une donnée qui permet de localiser une personne

Certaines informations (ex. le nom tout seul) ne suffisent pas à identifier une personne. On peut néanmoins parler de données personnelles lorsque la combinaison de telles informations permet à nouveau de reconnaître une personne (ex. le nom associé au prénom). Ce qui compte, c'est le fait de pouvoir effectivement identifier une personne.

! Attention ! Si une personne physique collecte ou utilise des données personnelles pour un **usage strictement personnel ou domestique** (ex. une liste d'invités non publiée), le règlement ne s'applique pas.

Qu'en est-il des métadonnées ?

Les métadonnées sont des informations supplémentaires sur des données. Ces informations décrivent la donnée et permettent ainsi de faciliter sa conservation ou consultation.
Exemple : les métadonnées par rapport à une photo pourraient être : la date, le lieu de la capture, le modèle de l'appareil photographique, etc.

Effectivement, les métadonnées peuvent constituer des données personnelles.

Le critère d'une donnée personnelle est l'identification. Si une personne n'est pas déterminée, elle peut néanmoins être identifiée par la combinaison de plusieurs données. Ainsi, des données initialement « non personnelles » deviennent personnelles.
Exemple : les données de géolocalisation relatives à une parcelle ne constituent en elles-mêmes pas des données personnelles. Si, en revanche, ces données sont combinées à un nom de famille et au nom d'une commune, il devient alors possible d'identifier une personne à l'aide de ce recoupement. Ces données, combinées entre elles, deviennent alors des données personnelles.

Selon la même idée, les métadonnées peuvent être considérées comme des données personnelles, si elles permettent l'identification d'une personne.

Quels sont mes droits ?

Droit d'information

Article 13 du règlement

Avant toute collecte d'une de vos données, vous devez être informé de cette collecte et de tous les droits qui en découlent.
L'information doit être claire et rédigée dans un langage compréhensible pour celui à qui elle est adressée.

Droit d'accès

Article 15 du règlement

Vous avez le droit d'obtenir à tout moment et **sans frais** une copie de toutes vos données personnelles détenues par un responsable (ex. dossier médical, dossier client, compte personnel sur un réseau social…). Il suffit de le contacter et d'en faire la demande.

! Attention ! En cas de demandes abusives (p.ex. lorsque vous demandez la délivrance d'une copie tous les mois), le responsable peut refuser votre demande ou bien exiger le paiement de certains frais.

Droit de rectification

Article 16 du règlement

Si vous constatez (lorsque vous exercez votre droit d'accès par exemple) que vos données personnelles sont inexactes ou incomplètes, vous pouvez demander directement au responsable de les rectifier ou compléter.

Droit à l'oubli : le déréférencement et l'effacement

Article 17 du règlement

Si vous tombez sur une information qui vous concerne, mais qui ne se justifie plus ou bien si vous souhaitez tout simplement que vos données personnelles détenues par un responsable disparaissent, vous avez deux possibilités :

- **Soit, vous demandez un « déréférencement » au moteur de recherche** (ex. Google)

Cela signifie qu'il n'est plus possible de trouver cette information parmi les résultats de ce moteur de recherche. L'information en elle-même ne sera pour autant pas supprimée !

Exemple : vous insérez votre nom dans le moteur de recherche et découvrez une photo de votre passé étudiant qui a été publiée sur le site de l'université. Vous pouvez alors demander un déréférencement au moteur de recherche. Si, à nouveau, vous insérez votre nom dans le moteur de recherche, vous ne trouverez plus la photo en cause parmi les résultats. En revanche, si vous vous rendez sur le site Internet de l'université, vous vous rendrez compte que la photo y figure toujours. Elle n'a pas été supprimée du site Internet, mais seulement des résultats du moteur de recherche.

La plupart des moteurs de recherche proposent des formulaires dédiés qu'il suffit de remplir en ligne : https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636558362364829420-2556796504&rd=1
(exemple de formulaire de Google)

- **Vous pouvez aussi demander l'effacement de la donnée directement au responsable qui la détient** (ex. par lettre ou par un formulaire proposé). L'information sera alors véritablement supprimée.

Est-ce que je peux faire effacer toutes mes données personnelles sans limite ?

Non. Le droit à l'oubli n'est pas infini.

- Il ne faut jamais oublier que n'importe quel internaute a pu faire une copie de votre donnée publiée sur Internet avant son effacement ou déréférencement. Il faut donc toujours être vigilant avant de publier des informations, des textes ou des images en ligne. Ce n'est pas pour rien que l'on dit : *Internet n'oublie jamais*…

- Ce droit connait des exceptions. Il n'est, par exemple, pas possible d'entraver la liberté d'expression et de la presse.

Exemple : Pierre est condamné pour vol. Quelques années plus tard, il se « googlise » lui-même. Dans ses recherches il tombe sur un article de presse en ligne qui concerne sa condamnation sans pour autant citer les noms. Mais, Pierre considère que le moteur de recherche fait expressément le lien entre cette condamnation et son nom. Il dépose une réclamation auprès de l'éditeur du journal et exige que l'information relative à la condamnation soit retirée de l'article. Dans ce cas, l'éditeur peut lui opposer sa liberté de la presse et peut laisser l'article en l'état.

Vous étiez mineur au moment de la communication de votre donnée (ex. un de vos parents a publié une photo de vous alors que vous étiez encore mineur) ?

Cette hypothèse est expressément prévue et soulignée par le RGPD. On peut donc considérer que les conditions pour l'exercice du droit à l'oubli concernant les données d'un mineur sont plus facilement remplies.

Droit à la limitation

Article 18 du règlement

Ce droit accompagne le plus souvent un de vos autres droits. Il vous permet d'interdire **temporairement** au responsable de traitement de continuer à utiliser vos données pendant une certaine période, et notamment jusqu'au moment où le responsable a vérifié l'exactitude des données (cf. droit de rectification), votre motif d'effacement (cf. droit d'effacement) ou d'opposition (cf. droit d'opposition).

! Attention ! Les données ne seront pas effacées, mais sont tout simplement « bloquées » temporairement dans le système du responsable.

Droit à la portabilité

Article 20 du règlement

Vous avez désormais le droit de demander au responsable de vous faire parvenir gratuitement les données, que vous lui avez fournies volontairement ou pour l'exécution d'un contrat, dans un format courant et lisible (ex. format .pdf). Vous pouvez également exiger qu'il transmette ces données directement à un autre responsable de votre choix (ex. en cas de changement d'un prestataire de service).

! Attention ! Cela ne signifie pas que vos données soient effacées ! Le responsable peut toujours continuer à les utiliser et vous pouvez toujours continuer à exercer vos droits auprès de lui (ex. droit à la rectification, droit à l'effacement).

Droit d'opposition

Article 21 du règlement

Dans certaines situations (ex. données utilisées à des fins de statistiques ou de prospection/publicité), vous pouvez vous opposer à la collecte ou l'utilisation de vos données.

Comment s'opposer concrètement ?

- La collecte de vos données suppose le plus souvent votre consentement. Vous pouvez alors tout simplement refuser de fournir des données personnelles.

Mon consentement n'est donc pas toujours nécessaire ? Non. Le responsable ne peut collecter et utiliser des données que si cela est fondé sur un socle de six bases légales que peuvent être le consentement de la personne concernée, mais également l'exécution d'un contrat, le respect d'une obligation légale, la sauvegarde des intérêts vitaux de la personne, l'exécution d'une mission d'intérêt public ou encore les intérêt légitimes du responsable.

! Attention !

Un site Internet a pré-coché une case (ex. la case « j'accepte les conditions générales », la case « j'accepte de recevoir des newsletter ») ? Dans ce cas, votre consentement n'est pas valide. Vous pouvez vous opposer encore plus facilement.

Vous avez moins de 16 ans et un site Internet vous adresse directement une offre ? Dans ce cas, votre consentement ne suffit pas. Le responsable doit en plus demander celui de vos parents.

- Si vous avez déjà fourni des données, vous pouvez informer directement le responsable (p.ex. par lettre) que vous retirez votre consentement pour l'avenir. Il n'aura alors plus le droit de vous envoyer des newsletters ou des publicités, par exemple.

Droit de s'opposer au profilage

Article 22 du règlement

Le profilage est un mécanisme automatisé qui analyse votre comportement afin de prédire des informations qui vous concernent (ex. situation financière, état de santé, préférences…).
Dès l'instant où le profilage vous affecte (ex. un système automatisé refuse de vous accorder un prêt), vous pouvez demander (dans certaines situations) à ce qu'une personne (et non plus une machine) analyse votre comportement. Vous avez en plus le droit de contester le résultat de cette analyse.

! Attention ! Le profilage ne devrait pas s'appliquer à des mineurs (de moins de 18 ans).

Qu'en est-il de la nouvelle « majorité » fixée à 16 ans ?

Le nouveau règlement estime que les enfants méritent une protection supplémentaire.

Est-ce que je suis désormais majeur sur Internet à partir de 16 ans ?

Non.

Le règlement exige dans certains cas votre consentement pour collecter vos données. Dans ce seul cadre, une personne de moins de 16 ans ne peut tout simplement donner son consentement à un **service sur Internet** qui lui est **directement offert**. Il faut le consentement du ou des titulaires de la responsabilité parentale, c'est-à-dire de vos parents. Un service sur Internet peut être un site de vente en ligne, une plateforme de streaming, un réseau social, etc.

! Attention ! Lorsque l'enfant utilise un forum ou un chat en ligne sous couvert de l'anonymat, aucune donnée personnelle n'est concernée et le règlement ne devrait pas s'appliquer. Par conséquent, le consentement des parents n'est pas requis, quel que soit l'âge de l'enfant.

En revanche, la qualité de donnée personnelle d'un pseudonyme est discutable.

Est-ce que cette limite d'âge de 16 ans s'applique dans tous les États ?

Le règlement permet à chaque État d'abaisser cette limite, qui ne pourra toutefois être inférieure à 13 ans. Si donc, vous avez moins de 13 ans, vous devez dans tous les cas demander le consentement de vos parents.

Pour l'instant, les États n'ont pas encore tous définitivement fixé cette limite. Il semble que le Luxembourg, comme d'autres pays européens, garde l'âge de 16 ans.

Comment les sites Internet vont-ils se conformer à cette majorité ?

Le règlement est souple et impose simplement au responsable de vérifier l'âge de l'internaute *« compte tenu des moyens technologiques disponibles. »*
A l'heure actuelle, il est difficile de prédire comment, et si véritablement, les entreprises vont vérifier à chaque fois l'âge de l'internaute et, le cas échéant, le consentement des parents.

Ce qui devrait sans doute être pris en compte dans l'effort raisonnable que doit faire le responsable, c'est le risque pour l'enfant. Plus le risque est élevé, plus les exigences sont fortes.

Que puis-je faire si mes droits ne sont pas respectés ?

1. Faire une démarche auprès du responsable de traitement ou du moteur de recherche

Il vaut toujours mieux essayer de régler votre litige à l'amiable.
Insistez auprès du responsable et informez-le de vos droits et de leur gratuité. Tout le monde n'est pas au courant de ce nouveau règlem ent. Souvent les grosses entreprises proposent des formulaires relatifs aux différents droits sur leurs sites Internet.

Exemple de formulaire pour le droit d'accès de Facebook :
https://fr-fr.facebook.com/help/226281544049399

Adressez-vous aux moteurs de recherche (Google, Yahoo, …), si vous souhaitez tout simplement qu'une information ne soit plus trouvable. En principe, ils mettent à votre disposition des formulaires dédiés et sont très favorables à de telles demandes.

Exemple de formulaire de déréférencement de Google :
https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636558362364829420-2556796504&rd=1

2. Introduire une réclamation auprès de la CNPD (article 77 du règlement)

Si vos démarches restent sans suites, vous pouvez introduire une réclamation auprès de la Commission nationale pour la protection des données (CNPD) qui met à votre disposition un formulaire dédié sur son site Internet :
https://cnpd.public.lu/fr/particuliers/faire-valoir/formulaire-plainte.html

3. Consulter un avocat et agir en justice

En dernier lieu, vous pouvez agir en justice afin de voir vos droits respectés et éventuellement obtenir la réparation de votre dommage matériel ou moral.
! Attention ! Avant de consulter un avocat, assurez-vous d'avoir pris toutes les autres mesures. Un procès peut être couteux et fastidieux.

Pour les curieux …

Le règlement ne s'est, bien évidemment, pas contenté d'améliorer les droits des personnes concernées, mais a également renforcé les devoirs de ceux qui collectent les données personnelles.
Principalement les devoirs des responsables de traitement s'articulent autour de trois nouveaux concepts.

Concept de l'accountability :

« *Accountability* », comme « *responsabilisation* », signifie que le responsable aura plus de responsabilité concernant vos données personnelles.

Pour mieux comprendre le concept, il est utile de connaitre la situation avant l'entrée en vigueur du règlement. Si une entreprise décidait de collecter des données, elle devait accomplir des formalités préalables ou obtenir une autorisation. Souvent, elle se sentait protégée par la suite et ne respectait pas forcément vos droits lors de l'utilisation de vos données.

Avec le nouveau règlement, une entreprise ne doit plus obtenir, en principe, d'autorisation. En revanche, elle doit être en mesure de prouver à tout moment qu'elle respecte l'intégralité du règlement. Concrètement, il ne suffit plus qu'elle demande votre consentement, mais elle doit, en plus, garder la preuve de ce consentement pendant toute la durée d'utilisation de votre donnée.

Concept de privacy by design :

Le responsable doit respecter vos données personnelles dès la création et la mise à disposition de son site Internet.

Concrètement, avant de créer un site, il doit réfléchir sur la manière de créer des fonctions permettant de recueillir votre consentement, de vous informer sur vos droits et de collecter vos données afin de rendre le site conforme au règlement.

Concept de privacy by default :

Les données personnelles sont protégées par défaut, c'est-à-dire sans qu'une action de l'internaute ne soit nécessaire.

Un site qui propose des cases pré-cochées ne respecte pas ce concept. En effet, sans action de l'internaute qui enlèverait la coche, les données personnelles sont collectées et le consentement n'est pas explicitement demandé (le « opt-out »). Bien au contraire, c'est le « opt-in » qui doit l'emporter (une case qui requiert le consentement de la personne concernée est vide et cette dernière la coche elle-même).

Mais le RGPD a également repris certains principes déjà existants. Ainsi, le responsable peut collecter des données personnelles, mais il doit respecter certaines règles.

Les principales règles sont les suivantes :

- **licéité, loyauté et transparence de la collecte** : le responsable doit respecter tous vous droits en collectant les données.
  Exemple : la collecte ne doit pas se faire à l'insu des personnes (cf. droit à l'information).
- **limitation des finalités** : le responsable doit indiquer clairement dans quel but il collecte la donnée et ne peut l'utiliser que pour ce but.
  Exemple : une école ne doit pas collecter des images d'élèves sous un prétexte administratif (constitution d'un dossier), pour ensuite les afficher dans un journal.
- **minimisation :** le responsable ne doit collecter que les données dont il a besoin pour accomplir le but indiqué.
  Exemple : Amazon ne devrait pas vous demander votre numéro de sécurité sociale pour effectuer un simple achat en ligne.
- **limitation de la conservation :** dès que le responsable a accompli son but, il ne doit, en principe, plus garder les données.
  Exemple : une école ne peut pas garder un dossier scolaire jusqu'à 30 ans après le départ de l'élève.

Que se passe-t-il si le responsable ne respecte pas ses devoirs ?

Une grande nouveauté du règlement consiste en l'augmentation de la sanction qui peut être prononcée à l'égard de celui qui ne respecte pas ses devoirs et vos droits.

Elle est passée à **20 millions d'euros ou 4% du chiffre d'affaires mondial.**

Cette peine élevée devrait contribuer à mieux responsabiliser les grosses entreprises multinationales.

Liens utiles

Pour recevoir des informations supplémentaires, vous pouvez consulter…
… le site de la CNPD : https://cnpd.public.lu/fr.html
… son guide pratique :
https://cnpd.public.lu/fr/publications/brochures/brochures/brochure-rt-st1.html

Sur le site de la commission nationale de l'informatique et des libertés française (CNIL), vous trouverez des modèles de lettres qui vous permettront d'exercer vos droits auprès du responsable. Ces modèles doivent bien évidemment être adaptés aux nouveaux numéros d'articles du règlement (état en avril 2018) :
https://www.cnil.fr/modeles/courrier

Pour des explications simples du RGPD en vidéo :
https://cnpd.public.lu/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees.html
https://www.youtube.com/watch?v=u4M5lVYv3UI
https://www.youtube.com/watch?v=KRZACR6GPVA

Pour une fiche pédagogique :
https://www.jedecide.be/sites/default/files/2018-01/Fiche%20p%C3%A9dagogique_0.pdf

Pour des explications simples et schématiques du RGPD : https://eugdprcompliant.com/

Ce document a un but purement d'information et ne remplace aucunement l'opinion d'un avocat après recherche et analyse juridique.

Pour toute question au sujet de l'arnaque en ligne ou sur l'utilisation d'Internet en général, contactez la BEE SECURE Helpline:

BEE SECURE HELPLINE CONSEIL Tél: 8002 1234

Editeur: BEE SECURE · B.P. 707 · L-2017 Luxembourg
Tel.: (+(+352) 247-86427 · Fax.: Fax: (+ 352) 46 41 86
bee-secure@snj.lu www.bee-secure.lu

BEE SECURE powered by Service National de la Jeunesse SECURITY MADE IN.LU kanner jugend telefon
Mee 18
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Co-financed by the European Union Connecting Europe Facility