LES LIVRES BLANCS NUAGEO

Comprendre le RGPD

N°3

Conseil Cloud | Nuageo

Sommaire

Avant-propos

L'objectif de ce livre blanc est de présenter le RGPD, son périmètre d'application et les nouvelles obligations qu'il impose aux entreprises pour établir un cadre juridique autour de l'utilisation des données personnelles. **Le point de vue présenté ici est celui des éditeurs et des entreprises, et non celui des particuliers** : ainsi, nous ne nous étendons pas sur les avancées en terme de portabilité des données et de consentement au traitement du point de vue du consommateur.

Le Règlement Général sur la Protection des Données entre en vigueur le 25 mai 2018. Ce règlement européen construit un cadre fort autour des données personnelles, depuis leur recueil jusqu'à leur destruction.

Dans ce livre, nous vous présentons le RGPD et ses conséquences, les mécanismes qu'il impose, et les outils à préparer pour sécuriser votre conformité.

Que vous soyez déjà dans les nuages, les pieds bien ancrés dans un datacentre, éditeur de service ou consommateur, le RGPD nous concerne tous.

Vous souhaitez estimer votre maturité RGPD ? Notre auto diagnostic, gratuit et rapide, peut vous aider.
Pour un accompagnement plus poussé, **GDPReady** est notre offre d'accompagnement sur le chemin de la conformité RGPD.

Nos livres blancs et autres publications sont à retrouver sur notre blog.

Posons les bases

Donnée personnelle

Une donnée personnelle est une donnée liée à une personne **physique**, et qui la caractérise.
Il s'agit donc classiquement du nom, prénom, adresse, adresse email, mais aussi la date de naissance, l'adresse IP...
En somme, tout information permettant d'identifier une personne physique directement ou indirectement.

Traitement

Le traitement est le terme retenu par le règlement pour désigner toute opération ou manipulation de données en vue d'une utilisation ultérieure. Il commence dès l'enregistrement d'informations au sein d'un outil particulier, même pour une utilisation ultérieure.

Ainsi, la création d'un tableau avec les noms/prénoms/adresses email pour servir de base à une campagne de visite constitue un traitement; la consignation de données personnelles au sein d'un outil CRM est un traitement; la réalisation de croisement sur les données personnelles afin d'établir des tendances sur les préférences de consommation d'un type de population (ce qui est désigné par "profilage" dans le RGPD) constitue aussi un traitement.

Par extension, le règlement concerne donc tout type de traitement, peu importe la visée de ce dernier : par exemple, même un traitement "Newsletter" entre dans le champ d'application, **qu'il soit à destination de particuliers ou de professionnels**, tant que ce traitement repose sur des données personnelles, telles que le nom ou l'adresse email.

Responsable de traitement, sous-traitant et autorité de contrôle

Le responsable du traitement, avant toute chose, est l'entreprise qui dispose des données et qui en souhaite l'utilisation.
Le sous-traitant est l'entreprise mandatée par le responsable de traitement pour effectuer le traitement concerné par le mandat, ou tout traitement nécessaire à l'accomplissement de la mission qui lui a été confiée par le responsable de traitement.

Il s'agit par exemple d'une entreprise (**responsable de traitement**) qui fait appel à un cabinet de conseil (**sous-traitant**) pour mener des campagnes de mails en masse.

L'**autorité de contrôle**, elle, est nationale, et compétente pour juger du respect du RGPD au sein des entreprises. Elle dispose de pouvoirs de contrôle et de sanction pour mener sa mission. Il s'agit du **point de contact pour le responsable de traitement** afin de valider sa conformité.
En France, cette autorité est la CNIL : la Commission Nationale Informatique et Libertés a la charge de veiller au respect des obligations imposées par le RGPD.

Co-responsabilité

Le RGPD précise une nouvelle relation de responsabilité entre le responsable du traitement, ses sous-traitants, et l'autorité de contrôle.

Avec le RGPD, cette relation est placée sous un **régime de co-responsabilité** : le responsable de traitement **ne pourra pas s'exonérer** de sa responsabilité en cas d'incident de sécurité lié aux données personnelles de la part du sous-traitant : il revient au responsable de traitement de choisir un sous-traitant présentant les garanties nécessaires en termes de respect du RGPD. Pour s'exonérer de toute responsabilité, le responsable de traitement devra prouver une faute du sous-traitant.
La réciproque vaut tout autant : charge au sous-traitant de prouver sa compétence et sa bonne foi par des preuves de son organisation et du respect du RGPD devant l'autorité de contrôle.

Inutile de trouver un responsable imaginaire, le responsable, c'est vous !

Quels critères d'application?

Au niveau des données

Les obligations de ce règlement concernent avant tout les données personnelles **générées sur le territoire européen**.

Ainsi, la nationalité de la personne concernée n'est pas un facteur discriminant : l'important est que la donnée soit produite sur un territoire de l'Union Européenne. Les législations nationales des ressortissants non européens importent peu ; si leurs données sont collectées en Europe (lors de vacances par exemple), leurs données sont de plein droit couvertes par le RGPD.

Par exemple, un ressortissant extra-communautaire qui s'inscrit sur un site e-commerce luxembourgeois sera donc concerné par ce règlement.

Au niveau des responsables de traitement

Ce règlement s'applique à tout responsable de traitement, établi dans l'Union Européenne ou non, qui traite des données relatives à un citoyen européen ou à un citoyen d'un autre pays dont les données ont été générées au sein de l'Union Européenne.

Ce règlement s'applique aussi aux sous-traitants établis en dehors de l'Union Européenne qui traitent des données de citoyens européens ou de citoyens d'un autre pays dont les données ont été générées au sein de l'Union Européenne.

Enfin, les sites Internet établis en dehors de l'UE, mais qui visent manifestement à adresser les citoyens européens sont aussi concernés : par **exemple, il peut s'agir d'un site établi aux Etats-Unis, dont l'interface est disponible en français, italien, espagnol, allemand et dont les prix sont affichés en euro**.

Les mécanismes prévus par le règlement

Des sanctions dissuasives

Une sanction en cas de manquement simple peut aller jusqu'à 2% du CA de l'entreprise (dans le cas d'une entreprise faisant partie d'un groupe international, il s'agit de 2% du CA du groupe) ou jusqu'à 10M d'euros.

En cas de faute grave, la sanction est doublée. Dans tous les cas, le montant le plus élevé est retenu.

L'autorité de contrôle nationale est chargée de statuer et d'émettre les sanctions lorsque cela est nécessaire.

Au-delà du préjudice financier, les répercussions seront les plus fortes au niveau de l'image de l'entreprise fautive. Car l'objectif de ce règlement n'est pas de punir la fuite de données, mais de prévenir les comportements à risque des entreprises peu regardantes des données personnelles.

Le registre d'activité, la base de connaissance des traitements

Le registre d'activité est un document listant l'ensemble des traitements menés par le responsable de traitement ou ses sous-traitants. Il est transmis à l'autorité de contrôle.

Son contenu

Le nom et les coordonnées du responsable du traitement, éventuellement son représentant, voire son Délégué à la Protection de la Donnée (DPD)
Lorsqu'il s'agit d'un sous-traitant en charge du traitement, les mêmes informations doivent apparaître.

La finalité du traitement
Par exemple : "Traitement visant la communication hebdomadaire de nos offres promotionnelles".

La description des catégories de personnes et des catégories de données personnelles
Par exemple : "Personnes ayant un historique de commande depuis l'établissement de l'entreprise" et "Traitement des données prénom et email".

Les catégories de destinataire des données
Par exemple : "Mailchimp pour l'envoi des communications".

Les documents attestant des garanties de sécurité appropriées
Par exemple : des résultats d'audit, des attestations provenant des éditeurs garantissant le respect de la confidentialité etc.

Si possible, la description des mesures appropriées
Il s'agit notamment d'illustrer la façon dont le responsable de traitement s'est structuré pour garantir le respect de la confidentialité des données.
Par exemple : l'illustration d'un processus avec les personnes en charge de chacune des actions, avec les responsabilités et les limitations d'accès aux données correspondantes.

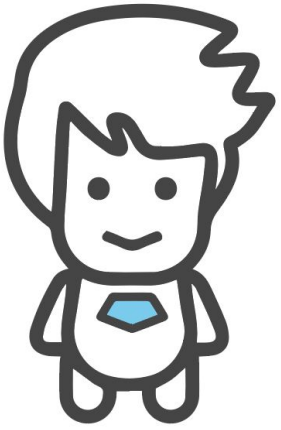
Les cas où il est obligatoire

- **Les traitement font courir un risque pour les droits et libertés des personnes** (la divulgation des résultats et des éléments sur lequel le traitement se base a des conséquences pour les individus dont les données sont traitées : fuite du couple login/mot de passe, de l'adresse mail ou physique,...)**.**
- **Les traitements concernent des données personnelles telles que visées à l'article 9 du règlement** (par exemple, des données relatives à la religion, l'ethnicité etc.).
- **Les traitements concernent des données personnelles visées par l'article 10 du règlement** (liées à des infractions et des condamnations pénales).
- **Les traitements ne sont pas occasionnels**, c'est à dire qu'ils sont réguliers dans le temps.

A noter que les entreprises de moins de 250 employés sont dispensées d'une telle obligation. Pour autant, il reste très vivement conseillé.

Le DPD, superhéros des données personnelles en entreprise

L'article 37 du règlement le précise, le DPD (Délégué à la Protection des Données ou Data Privacy Officer en anglais, DPO) est obligatoire dans les cas où :



- **Le responsable de traitement est une autorité ou un organisme public.**
- **Les activités de base du responsable de traitement (ou du sous-traitant) par leur nature, leur portée ou leur finalité demandent un suivi régulier.** *Par exemple, une entreprise offrant des biens ou des services à la vente du public (B2C ou B2B2C).*
- **Les activités de base du responsable de traitement (ou du sous-traitant) consistent en un traitement de données à grande échelle, ou concernent les données visées par l'article 9 ou 10.** *Par exemple, une entreprise spécialisée dans le traitement de données statistiques.*
- **Dans les autres cas, il n'existe pas de contrainte posée par le règlement ; cette contrainte peut en revanche être créée par la loi nationale.**

Le DPD n'est donc pas obligatoire; il reste vivement conseillé car sa mission au sein de l'entreprise est d'apporter une assistance et un conseil au responsable de traitement pour garantir le respect des obligations portées par la RGPD.

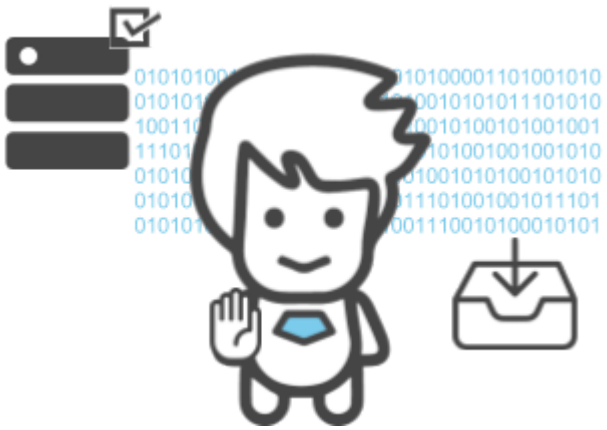
Le DPD doit en revanche présenter des qualités professionnelles et des connaissances juridiques le rendant apte à l'accomplissement de cette mission. Si vous disposez d'un Correspondant Informatique et Libertés, c'est le profil parfaitement adapté à cette mission.

D'une façon générale, le DPD doit être indépendant dans sa mission de conseil interne : il ne doit recevoir aucune instruction concernant l'exercice de ses missions, afin d'apporter le regard critique nécessaire quant au respect du RGPD.

Enfin, un dernier point : il n'existe aucune obligation sur l'emploi à plein temps du DPD, ou de son exclusivité. Il est explicitement prévu que le DPD peut être nommé au nom de plusieurs entreprises, à condition qu'il soit facilement joignable par chacune des entreprises. De même, il peut s'agir d'une personne mandatée par un contrat de service.

L'approche *privacy-by-default* sacralisée

Les services manipulant des données personnelles devront basculer sur une conception et un fonctionnement reposant sur l'utilisation parcimonieuse des données personnelles.



C'est à dire que ces services devront utiliser uniquement les données strictement nécessaires, afin de limiter aussi bien les risques en cas d'incidents qu'une utilisation non autorisée de ces données.

C'est dans ce cadre-là que le DPD doit notamment apporter son expertise, pour encadrer l'utilisation de ces données et le respect des consentements accordés par les utilisateurs.

Toujours dans le cadre de cette approche, les entreprises devront mettre en oeuvre des mécanismes pour limiter l'accès aux données personnelles par des personnels non autorisés, et les documenter.

Enfin, le règlement précise bien que le responsable de traitement doit garantir la sécurité du traitement…en fonction des coûts et des risques.

Les données hébergées en Europe et ailleurs, sous conditions

Le règlement n'impose pas, stricto sensu, la domiciliation des données au sein de l'Union Européenne. En revanche, il est demandé d'héberger les données personnelles au sein de pays proposant le même niveau de garantie que l'Union Européenne.

Pour cela, le règlement identifie trois cas :

1. **L'hébergement des données personnelles au sein de l'Union Européenne** : même si ce n'est pas imposé, il s'agit de la solution la plus naturelle.
2. **L'hébergement des données au sein d'un pays reconnu par l'Union Européenne comme offrant le même niveau de garantie d'un point de vue sécurité/confidentialité** : ce cas est particulièrement illustré par le traité avec les Etats-Unis, connu sous le nom du Privacy Shield.
3. **L'hébergement des données au sein d'un pays tiers, avec un contrat spécifique (comprenant notamment les Binding Corporate Rules)** : il est du ressort de l'entreprise d'encadrer la relation avec l'hébergeur de façon à proposer un cadre contractuel permettant la garantie du traitement des données personnelles selon le cadre imposé par le règlement.

Un commentaire sur ce point : il s'agit d'une excellente mesure pour ne pas bloquer les entreprises dans leur utilisation des outils Cloud. En revanche, une réflexion de fond doit être menée : **quel est le cadre juridique réel en vigueur à l'endroit où mes données sont hébergées?**

L'analyse d'impact comme préalable à tout traitement

Le règlement établit clairement que l'utilisation de technologies avancées pour le traitement de données personnelles doit faire l'objet d'une analyse d'impact. Cette analyse d'impact doit permettre au responsable de traitement d'identifier les risques portant sur les traitements qu'il effectue, et donc les mesures de sécurisation à mettre en oeuvre pour sécuriser ces traitements.

Parmi ces technologies, on peut penser par exemple et de façon non exhaustive :

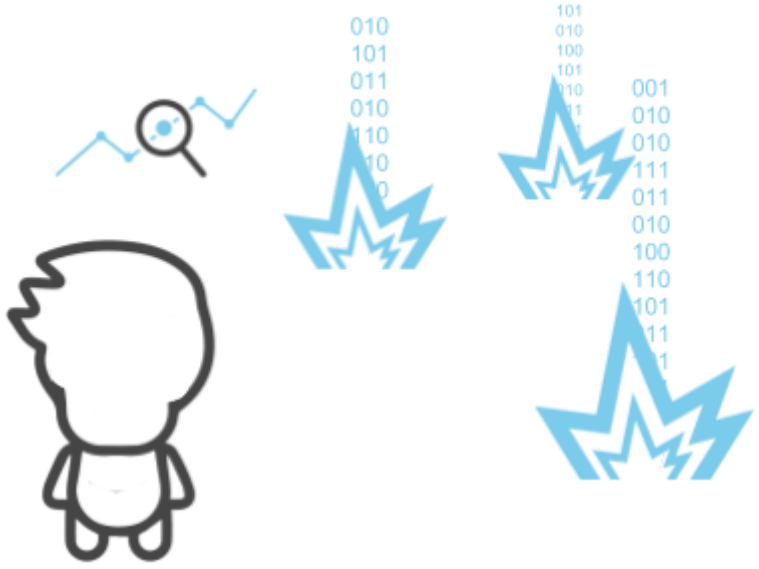
- Au **machine learning,** par exemple sur les données de comportement des internautes sur un site e-commerce pour l'envoi de newsletters automatisées sur leurs centres d'intérêts (par l'agrégation des données, des profils de consommateurs sont établis sur la base des informations personnelles et de comportements de consommation).
- A l'**intelligence artificielle** pour la reconnaissance de personnes.
- Au **big data** pour le profilage des personnes.

D'une façon plus générale, il est entendu dans le règlement que ces analyses d'impact doivent être menées par le Délégué à la Protection des Données (le Data Privacy Officer pour les anglophones).

Cette analyse d'impact doit avoir lieu dès la conception du service ou, le cas échéant, dès l'étude du déploiement pour le responsable de traitement.

Il est à noter que cette analyse d'impact doit également être menée sur des services ou procédés existants, dès lors qu'ils font peser un risque sur les droits et libertés des personnes dont les données personnelles sont manipulées.

Par exemple, les procédés actuels quant au traitement de la paie doivent faire l'objet d'une telle analyse.



Anticipez les impacts, ne vous laissez pas surprendre !

Le rôle des guides de bonnes pratiques et des codes de conduite

Le règlement propose des pistes pour améliorer la confidentialité et la sécurité des traitements, mais ne propose pas de méthode “prête à l’emploi”.

Que ce soit pour le responsable du traitement, pour ses sous-traitants, ou pour les autorités nationales, la question des bonnes pratiques et des certifications est prégnante :

Le responsable du traitement doit, dans la mesure du possible, suivre les codes de conduite liés au traitement des données personnelles.

Pour un sous-traitant, le suivi de ces bonnes pratiques est un élément différenciant pour établir sa pertinence auprès d’un responsable de traitement.

L’autorité de contrôle doit valider ces codes de conduite, et certifier les entreprises quant au bon traitement des données personnelles.

Le véritable enjeu va cependant plus loin : en cas d’incident de sécurité lié aux données personnelles, le responsable de traitement doit être en capacité de prouver qu’il a mis en oeuvre les moyens adéquats pour sécuriser le traitement des données personnelles ; le suivi de codes de conduite et les certifications participent à cette démarche.

Cela permet de renforcer la confiance des utilisateurs : aujourd’hui, il existe une dérive profonde sur l’utilisation des données personnelles ; demain, en mettant en avant le suivi de bonnes pratiques, librement consultables, les entreprises peuvent promouvoir une attitude responsable et ouverte avec leurs utilisateurs, ce qui offre un vrai vecteur de différenciation.

A ce jour, ces bonnes pratiques sont à construire. Il est essentiel qu’utilisateurs et éditeurs avancent en coopération pour identifier les bonnes pratiques et fédérer les acteurs autour de ces dernières.

Une transparence renforcée du responsable du traitement

Le RGPD précise le droit des personnes vis à vis de leurs données et établit de nouvelles obligations pour les responsables de traitement :

Relation avec l'autorité de contrôle

Le responsable de traitement doit globalement être plus transparent dans sa relation avec l'autorité de contrôle, notamment lors de la survenance d'incidents liés aux données personnelles.

En effet, l'article 55 précise que le responsable de traitement doit, dans un délai de 72 heures après avoir pris connaissance de la survenance d'un incident lié aux données personnelles, informer l'autorité de contrôle.

Recueil explicite du consentement pour chaque traitement

Avant que des données personnelles ne soient collectées, le responsable de traitement doit recueillir le consentement des personnes de façon explicite pour chacun des traitements qui seront effectués. Il doit être en capacité de prouver à l'autorité de contrôle qu'il dispose du consentement clairement exprimé de chacune des personnes dont il traite les données, sous peine de sanction.

Ce consentement peut être donné sous diverses formes : consentement écrit, case à cocher etc. L'essentiel est que la demande de consentement présente clairement la portée et la finalité du traitement, la durée de conservation des données, et que la personne dispose du droit de retirer son consentement ultérieurement.

Un point à noter : si le consentement a été recueilli sous une forme correspondant à la directive européenne 2002/58/CE, ou au sens de la loi Informatique et Libertés (qui fait la transposition de la directive européenne 2002/58/CE), il n'est pas nécessaire de le recueillir à nouveau.

Exception notable : il est à noter que les données traitées pour la réalisation du contrat passé entre l'entreprise et l'utilisateur ne font pas l'objet de ce consentement préalable. Il s'agit par exemple des données nécessaires à la livraison d'une commande sur un site e-commerce.

Gestion des données personnelles

Le responsable de traitement est tenu d'organiser et de prévoir les cas où une personne demanderait la rectification des données dont il dispose et les traitements effectués sur celles-ci, mais aussi leur portabilité vers un autre responsable de traitement.

Toute personne peut ainsi demander l'accès, la modification, la rectification ou la suppression des données qui lui sont relatives, à condition de prouver son identité de façon indiscutable au responsable de traitement. Si une modification des données survient du fait du responsable de traitement, il est tenu d'en notifier l'ensemble de la chaîne de traitement.

Concernant la portabilité des données, elle doit être organisée autour d'un format de donnée couramment utilisé et lisible par machine.

Communication en cas d'incident

En cas d'incident, le responsable de traitement a l'obligation d'informer les personnes dont les données auraient été compromises. Cette communication doit comprendre les coordonnées du Délégué à la Protection des Données, le type d'incident, les conséquences probables consécutifs à l'incident et les mesures prises pour résoudre les causes de l'incident et diminuer les conséquences négatives.

Conclusion

Dans les faits, le Règlement Général sur la Protection des Données s'applique à tous, et plus particulièrement à des entreprises qui ne sont pas préparées à adresser ces nouveaux enjeux.

Si les chantiers à mener sont nombreux, il s'agit avant tout de **mettre en oeuvre une culture et une organisation centrée sur l'utilisation raisonnée et encadrée des données personnelles**.

L'objectif poursuivi par le RGPD n'est pas la sanction aveugle des contrevenants et des entreprises n'ayant matériellement pas pu se mettre en conformité au 25 mai 2018, mais bien de susciter une prise de conscience autour des données personnelles, qui constituent la ressource principale de l'écosystème digital.

Au-delà des sanctions, au-delà des nouvelles obligations, le RGPD pose un cadre cohérent au niveau européen et mondial pour l'exploitation des données personnelles. Nulle organisation n'est exemptée de suivre ce règlement tant que les données sont d'origine européenne (de par leur source ou de par la citoyenneté de la personne physique).

Il s'agit d'une opportunité de faire table rase d'un passé marqué par les abus, et de regagner la confiance des utilisateurs.

Êtes-vous **GDP*R****eady*** ?

ps : En cas de doute, notre auto diagnostic, gratuit et rapide, peut vous aider.

Société de conseil spécialisée dans la transformation numérique des entreprises

Nuageo.fr