FAQ - RGPD

FAQ basée sur celle du site de la d.a.n.e de Lyon (source)

Le RGPD en bref, c'est quoi ?

Le RGPD est la nouvelle réglementation européenne en matière de protection des données des personnes physiques. Il fait suite à la Loi Informatique et Libertés, qui reste pleinement en vigueur, mais remplace la Directive 95/46/CE relative à la protection des données personnelles.

L'arrivée du RGPD, fait disparaitre la nécessité des démarches auprès de la CNIL ; RGPD vise à responsabiliser les acteurs économiques détenant des données personnelles.

Tout traitement de données (voir plus loin) au sein de l'entreprise devra être répertorié dans un registre, maintenu à jour par le Délégué à la Protection des Données (DPD - ou *DPO* en anglais : "*Data Protection Officer*"). Les éventuels contrôles du caractère correct et exhaustif de ce recensement ont vocation à être effectués par le personnel de la CNIL.

Quels sont les grands principes ?

Le RGPD est organisé pour garantir 3 grands principes :

1. Gestion responsable (*Accountability*)
RGPD vise à *responsabiliser* l'entreprise "responsable de traitements". Cela consiste tout simplement pour le DPO à documenter tous les traitements de Données à Caractère Personnel (DCP), et tenir cette documentation constamment à jour. Le DPO doit sensibiliser les équipes sur ce thème et mettre en place les procédures internes appropriées.

2. Protection des données dès la conception des systèmes (*Privacy by design*)
L'idée est de protéger les données dès la conception des services/systèmes qui

vont les manipuler. C'est d'ailleurs dans cette optique que les services R&D devront désormais associer leur DPO dès le début des réflexions sur des développements portant sur de nouvelles fonctionnalités.

3. Protection des données par défaut (*Privacy by default*)
Il s'agit de limiter la quantité de DCP traitées, leur accessibilité et leur durée de conservation : seules seront stockées les DCP réellement nécessaires à la finalité d'un traitement précis.

Une DCP, c'est quoi ?

Depuis la Loi n° 2004-801 du 6 août 2004, on ne parle plus d'informations « nominatives » (Loi n° 78-17 du 6 janvier 1978), mais de "Données à Caractère Personnel" (ou DCP). Est considérée comme une DCP, toute information permettant de faire le lien directement ou indirectement avec une personne physique. Le texte ne précise pas le type de support concerné (numérique ou papier) :

« *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. 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.* » (art. 2).

Concrètement, une donnée à caractère personnel peut être un nom, un prénom, une date de naissance, mais aussi un pseudonyme, un numéro de sécurité sociale, une plaque d'immatriculation de véhicule, un numéro de téléphone, une adresse IP, un historique de navigation, une géolocalisation, une photographie, un avatar, etc.

Concrètement, le RGPD, ça change quoi vis-à-vis de la CNIL ?

A partir du 25 mai 2018, il n'y a plus lieu dans les entreprises d'engager une quelconque démarche de déclaration à la CNIL. Les entreprises inscrivent désormais les traitements de DCP dans leur registre, tenu par leur DPO ("*Data Protection Officer*").

Quelques exceptions cependant : les démarches déclaratives auprès de la CNIL restent d'actualité pour le traitement de données dites *sensibles* aux termes de la Loi 1978, comme par exemple les données *biométriques*.

Le RGPD, ça concerne qui ?

Le service public
Les établissements scolaires, les collectivités locales, les hôpitaux, les universités… bref, toutes les entités juridiques du service public.

Les entreprises
Dans le secteur privé, cela concerne *toutes* les entreprises, mais seules celles dont le nombre d'employés est supérieur à 250 ou celles, quelle que soit leur taille, qui traitent des données *sensibles* comme par exemple des données médicales patients, ont obligation de tenir un registre (cf article 30-5 ci-dessous) :

"*[C]es obligations (...) ne s'appliquent [en général] pas à une entreprise ou à une organisation comptant moins de 250 employés.*"

Qu'est-ce qu'un "traitement" ?

Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...)

Qui est le responsable du traitement des données ?

Le responsable du traitement est 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 des données personnelles concernées.

Un DPO, c'est quoi ? Quel est son rôle ?

Le DPO (Data Protection Officer), est une personne chargée d'assurer la conformité et la sécurité des traitements au sein de l'entité pour laquelle il bénéficie d'une délégation de responsabilité sur le sujet.

Le DPO veille à l'intégrité et à la protection des DCP (Données à Caractère Personnel) de son entité, tant sur le plan juridique que technique. Il fait également le lien entre son entité et l'autorité de contrôle (la CNIL).

Il recense tous les traitements de données à caractère personnel de l'établissement, prépare des procédures spécifiques, sensibilise le personnel de son entreprise ...

Quel est le profil idéal du DPO ?

Selon la CNIL, le DPO remplissant un rôle transversal doit être un « très bon communicant ». En plus des aspects techniques, juridiques et éthiques, le DPO doit parfaitement connaître les enjeux métiers ; il ne doit en aucun cas être un frein au développement de nouveaux usages mais sensibiliser son organisation à ce que ces nouveaux usages vont impliquer en regard du RGPD. Le DPO a un rôle fort d'orientation à jouer ; il contribue à la dynamique et à l'image de l'entreprise. Il est recommandé de l'associer au plus haut dans l'organigramme, et lui donner un rôle central, nécessaire à l'accomplissement de ses missions.

Le DPO peut tout aussi bien exercer par ailleurs dans l'entreprise un métier comme celui de référent numérique, responsable administratif, enseignant, informaticien ... Le DPO doit surtout être une personne qui communique, et qui sait gagner la confiance de ses interlocuteurs - même si de bons réflexes concernant le cadre juridique applicable aux données à caractère personnel restent indispensables (des actions de formation peuvent être à prévoir sur ce sujet, le cas échéant).

Est-on obligé de nommer un DPO ?

Oui. Chaque responsable de données a obligation légale de nommer un DPO. La nomination d'un DPO devra d'ailleurs être déclarée auprès de la CNIL via un formulaire en ligne.

A noter également qu'il est possible de faire appel à un prestataire externe, pour assurer cette mission de DPO, et/ou de mutualiser un même DPO pour un groupement d'entreprises.

Peut-on mutualiser un DPO entre plusieurs entreprises ?

Oui. L'article 37-3 autorise tout à fait la désignation d'un DPO pour plusieurs entités. Cette mutualisation est même conseillée par le législateur, dans la mesure où il sera peut-être parfois difficile de trouver une personne compétente dans chaque entreprise.

A-t-on le droit de faire appel à un prestataire de services pour assurer le rôle du DPO ?

Oui. L'article 37-6 autorise les responsables de traitements des données à faire appel à des sociétés externes pour assurer les missions de leur DPO.

Le DPO peut-il être tenu responsable d'un manquement au RGPD ?

Non. Ultimement, la responsabilité du respect du RGPD reste entièrement du ressort du responsable de traitement des données ; dans l'organisation, le DPO a en revanche l'obligation de sensibiliser, et le cas échéant d'alerter ce dernier s'il identifie des risques de non-conformité avec le règlement.

Un délai de 72h est par exemple prévu pour signaler à la CNIL la découverte de toute violation de données personnelles, comme par exemple une faille de sécurité qui aurait entrainé la divulgation ou la perte de données personnelles.

Comment savoir si les inscriptions au registre de l'entreprise sont conformes ?

Les personnes désignées CIL (Correspondants Informatique et Liberté) jusque-là ayant vocation à devenir DPO le 25 mai 2018, la liste actuelle gérée par la CNIL et à destination des CIL (ou équivalente) sera utilisée pour les DPO, afin qu'ils puissent poser des questions pour se renseigner et parfaire leurs connaissances.

Concrètement tous les traitements en place dans l'entreprise et portant sur des données sensibles (telles que des données médicales, relatives à l'orientation sexuelle, aux convictions religieuses, philosophiques, politiques, etc.) doivent figurer dans le registre des traitements de cette dernière.

« Cartographie » et « inscription au registre » : c'est la même chose ?

Non. Ces deux notions correspondent à deux étapes à franchir pour permettre la mise en conformité des traitements de l'entreprise. Il faut *d'abord* recenser tous les traitements actuels et envisagés (c'est ce qu'on appelle la cartographie des traitements), *puis* faire une analyse d'impact sur la vie privée de ces traitements (ou « PIA » en anglais, pour Privacy Impact Assessment). Voir par exemple les documents d'accompagnement prévus par la CNIL. L'inscription d'un traitement de DCP au registre du DPO doit se faire pour les traitements qui sont déclarés conformes.

Comment s'y prendre pour réaliser la cartographie des traitements ?

On distingue six points de vigilance pour une cartographie efficiente des traitements de données personnelles. Il convient pour ce faire de se poser les questions suivantes :

1. Qui gère ce traitement ?
Pour cela, l'entreprise doit inscrire le nom du responsable de traitement ou celui du DPO, identifier les responsables qui traitent les données à l'intérieur de l'entité et dresser la liste des sous-traitants.

2. Quel type de données personnelles est traité ?
Il s'agit ici de recenser les différents types de données traitées et celles qui présentent un risque éventuel pour la vie privée des personnes concernées par le traitement.

3. Quel est l'objectif du traitement des données ?
Il convient de préciser la finalité principale du traitement.

4. Par où transitent les données personnelles ?
Le RGPD impose d'indiquer la localisation de l'hébergement des données traitées, y compris lorsqu'il y a transfert de données hors Union Européenne (UE).

5. Pendant combien de temps seront stockées les données ?
Il convient de préciser le temps de conservation de ces données.

6. Quelles sont les mesures de sécurité mises en place ?
Le responsable des traitements doit déterminer toutes les données à risque et les mesures prises pour en garantir la sécurité. Il faut aussi engager des études d'impact sur la vie privée des personnes, lorsque c'est nécessaire, afin de mesurer le risque éventuel qui serait supporté si ces données étaient divulguées ou détruites.

Quelles sanctions en cas de non- respect du RGPD par l'entreprise ?

La CNIL est chargée de veiller au bon respect de la protection des données, et a autorité pour prononcer des amendes pouvant aller jusqu'à 20 millions d'euros, ou 4% du chiffre d'affaire mondial de l'entreprise ou du groupe d'entreprises, en cas de manquement au règlement.

Pour aller plus loin dans la connaissance du RGPD …

- FAQ RGPD sur le site de la CNIL
- Le CIL et le futur délégué à la protection des données
- Règlement européen : se préparer en 6 étapes
- 6 fiches CNIL pour se préparer au RGPD
- DPO : un gardien pour les données personnelles
- Le principe d'« Accountability » ou comment passer de la théorie à la pratique
- Règlement européen sur la protection des données : ce qui change pour les professionnels
- Devenir délégué à la protection des données
- Cartographier les données personnelles
- Le RGPD modélisé
- La CNIL conseille pour la cartographie des traitements