https://dane.ac-lyon.fr/spip/FAQ-RGPD-Reglement-General-pour-la

FAQ RGPD (Règlement Général pour la Protection des Données)

- Se former - Cadre juridique -

Date de mise en ligne : vendredi 27 octobre 2017

Vous pouvez également nous poser vos questions directement sur Twitter (@DANE_acLyon), notamment afin d'enrichir cet article.

Foire Aux Questions (non exhaustif)

1. Le RGPD, c'est quoi ?

Le RGPD est la nouvelle réglementation européenne en matière de protection des données, et fait suite à la loi informatique et libertés, qui reste pleinement en vigueur, remplace la directive 95/46/CE sur la protection des données personnelles.

Avec le RGPD, c'est aussi la disparition des démarches CNIL, afin de simplifier et responsabiliser. Tout traitement de données au sein de l'établissement (élèves et personnels) devra être inscrit sur un registre, et maintenu à jour par le Délégué à la Protection des Données (DPD - ou *DPO* en anglais : "*Data Protection Officer*"). Les éventuels contrôles seront effectués par la CNIL.

2. Quels sont les grands principes ?

Le RGPD est organisé autour de 3 grands principes :

1. Gestion comptable (*Accountability*)
Le principe de gestion comptable vise à responsabiliser le responsable des traitements. Cela consiste tout simplement à documenter tous les traitements de DCP, et de les tenir constamment à jour. Le DPD doit donc sensibiliser et mettre en place des procédures internes (cf article 5 du RGPD).

2. Protection des données dès la conception (*Privacy by design*)
L'idée est de protéger les données dès la conception des services. C'est d'ailleurs dans cette optique, que les enseignants devront associer leur DPD dès le début aux réflexions pédagogiques, dans le cadre de la construction d'activités (cf article 25 du RGPD).

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 les DCP nécessaires au fonctionnement, pour ne garder que le strict nécessaire en fonction de la finalité du traitement. (cf article 25 du RGPD).

3. 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 (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.

Plus d'informations sur Jurispedia :

4. Concrètement, le RGPD, ça change quoi ?

A partir du 25 mai 2018, il n'y a plus de démarche CNIL dans les établissements. Ce sont les établissements eux-mêmes qui inscrivent les traitements de DCP dans un registre tenu par le DPD (Délégué à la Protection des Données, ou DPO en anglais "*Data Protection Officer*").

Quelques exceptions cependant : les démarches déclaratives auprès de la CNIL restent d'actualité pour le traitement de données dites sensibles au terme de la Loi 1978, comme par exemple les données biométriques (les empreintes digitales pour le passage à la cantine en sont une excellente illustration).

5. 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 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.*"

6. Qui est le responsable du traitement des données ?

Pour les **collèges et les lycées**, le responsable du traitement des données est le chef d'établissement (privé ou public).

Dans le **premier degré**, pour les écoles maternelles et élémentaires publiques, le responsable des traitements est le DASEN du département (en effet, ni les directeurs d'école, ni les IEN n'ont le statut de personnes morales). Pour les écoles privées, il s'agit du directeur d'école, étant donné que les écoles privées ont le statut d'association loi 1901.

(cf article 5 de l'arrêté du 13 octobre 2017 sur Légifrance)

Pour le **Rectorat**, le responsable du traitement des données est le recteur.

7. Un DPD, c'est quoi ? Quel est son rôle ?

Le DPD (Délégué à la Protection des Données), ou *DPO* en anglais (*Data Protection Officer*), est une personne chargée d'assurer la conformité et la sécurité des traitements au sein de l'entité pour laquelle il a délégation de responsabilité.

Le DPD 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 les agents...

8. Quel est le profil idéal du DPD ?

Le DPD a un rôle transversal, et doit être un Â« *très bon communicant* Â», d'après la CNIL. En plus des aspects

techniques, juridiques et éthiques, le DPD doit parfaitement connaître les enjeux métiers, et ne doit en aucun cas être un frein au développement des usages. Le DPD a un rôle politique à jouer ; il contribue à la dynamique et à l'image de l'établissement, et il est conseillé de l'associer au plus haut dans l'organigramme, et lui donner le rôle central nécessaire à ses missions.

Le DPD peut aussi bien être référent numérique, responsable administratif, enseignant, informaticien... Le DPD doit surtout être une personne qui communique, et qui sait gagner la confiance de ses collaborateurs - même si de solides connaissances sur le cadre juridique sur le champ des données à caractère personnel restent indispensables (des actions de formations peuvent être à prévoir).

9. Est-on obligé de nommer un DPD ?

Oui. Chaque responsable des données a obligation légale de nommer un Délégué à la Protection des Données (ou *DPO* en anglais : "*Data Protection Officer*"). La nomination d'un DPD 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 la mission de DPD, et/ou de mutualiser un même DPD pour un groupement d'établissements.

Article 37 du RGPD, relatif à la désignation du délégué à la protection des données.

10. Le DPD peut-il être tenu responsable d'un manquement au RGPD ?

Non. La responsabilité du respect du RGPD revient entièrement au responsable du traitement des données ; le DPD a en revanche obligation de sensibiliser, et le cas échéant d'alerter ce dernier.

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

11. Quelles sanctions en cas de non respect du RGPD ?

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 en cas de manquement au réglement.

12. Comment savoir si les inscriptions au registre sont conformes ?

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

13. Peut-on mutualiser un DPD pour plusieurs établissements ?

Oui, l'article 37-3 autorise la désignation d'un DPD pour plusieurs organismes. Cette mutualisation est même conseillée dans la mesure où il sera peut-être parfois difficile de trouver des personnes compétentes dans tous les établissements.

14. A-t-on le droit de faire appel à un prestataire de services pour le DPD ?

Oui, l'article 37-6 autorise les responsables de traitements des données à faire appel à des sociétés externes pour assurer les missions de DPD.

15. Cartographie et inscription au registre : c'est la même chose ?

Non, mais ce sont deux étapes nécessaires pour permettre la mise en conformité des traitements. Il faut d'abord recenser tous les traitements actuels et envisagés (c'est ce qu'on appelle la cartographie des traitements, qui peut par exemple se faire sous forme de carte mentale), puis faire une analyse d'impact sur la vie privée (ou Â« PIA Â» en anglais, pour Privacy Impact Assessment). Voir par exemple lesdocuments d'accompagnement prévus par la CNIL, ou encore le logiciel open source). L'inscription d'un traitement de DCP au registre du DPD se fait pour les traitements qui sont déclarés conformes.

16. Comment s'y prendre pour la cartographie des traitements ?

On distingue six points de vigilance pour une cartographie efficiente d'un traitement de données. 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 DPD, identifier les responsables qui traitent les données à l'intérieur de l'entité et rédiger 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. Cela peut par exemple servir à permettre un suivi d'apprentissage, ou l'utilisation de services en ligne à but pédagogique.

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

5. Combien de temps sont stockées les données ?
Il convient également 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 risques. Il faut bien-entendu engager des études d'impact sur la vie privée des personnes lorsque c'est nécessaire, afin d'assurer le plus haut niveau de sécurité pour chaque traitement

Pour aller plus loin

- 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
- DPD : 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
- Le DPD : définition, formation et salaire (secteur privé)
- Les labels CNIL
- Le RGPD en datavisualisation interactive.
- Cartographier les données personnelles
- Le RGPD modélisé
- La CNIL conseille pour la cartographie des traitements
- Tout savoir sur le RGPD (Blog du Modérateur)

Cf aussi l'article Â« *Historique de la protection des données en France* Â».

Glossaire

- CIL : Correspondant Informatique et Liberté
- CNIL : Commission Nationale de l'Informatique et des Libertés
- DASEN : Directeur académique des services de l'Éducation nationale
- DCP : Donnée(s) à Caractère Personnel
- DPD : Délégué.e à la Protection des Données (ou DPO en anglais)
- DPO : Data Protection Officer (ou DPD en français)
- G29 : Groupe de travail Article 29 sur la protection des données (CNIL européennes)
- IEN : Inspecteur de l'Education Nationale
- INA : Institut National de l'audiovisuel
- INSE : Institut national de la statistique et des études économiques
- RGPD : Réglement Général pour la Protection des Données
- SAFARI : Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus