LES NOTES DE L'UNION DESMAIRES

LE RÈGLEMENT GÉNÉRAL DE PROTECTION DES DONNÉES

R.G.P.D.

LE RÈGLEMENT GÉNÉRAL DE PROTECTION

DES DONNÉES

R.G.P.D.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) (ce texte est disponible sur le site de la CNIL)

Cette nouvelle législation complète la loi informatique et liberté de 1978 et la loi république numérique (LRP) en créant de nouveaux droits et obligations.

- ✓ QUELQUES ÉLÉMENTS PRÉLIMINAIRES
- ✓ QUE RÉGIT LE R.G.P.D. ?
- ✓ QUELLES SONT LES DONNÉES Á CARACTÈRE PERSONNEL ?
- ✓ QUE RECOUVRE LE TRAITEMENT DES DONNÉES ?
- ✓ QUEL EST LE RÔLE DE L'AUTORITÉ DE PROTECTION DES DONNÉES ?
- ✓ QUID DES ADMINISTRATIONS PUBLIQUES ?
- ✓ 6 ÉTAPES RECOMMANDÉES PAR LA CNIL

Quelques éléments préliminaires

Quelques précisions utiles

- ✓ **Le Règlement sera applicable à partir du 25 mai 2018 (art 99.2) dans tous les pays de l'Union Européenne**
- ✓ **Ils s'applique à toutes les entreprises, les administrations et les associations qui traitent des données à caractère personnel**
- ✓ **Les fichiers déjà mis en œuvre à cette date devront, d'ici là, être mis en conformité avec le règlement.**

Que régit le R.G.P.D. ?

Le R.G.P.D. concerne qui et quoi ?

Le nouveau règlement général sur la protection des données ("RGPD") réglemente le traitement par une **personne, une entreprise ou une organisation** des **données à caractère personnel** concernant des **personnes** au sein de l'UE.

Il ne s'applique pas au traitement des données à caractère personnel **des personnes décédées ou des personnes morales.**

Les règles ne s'appliquent pas aux données traitées par une personne à des fins purement personnelles ou dans le cadre d'une activité domestique, à condition qu'il n'y ait aucun lien avec une activité professionnelle ou commerciale. Lorsqu'une personne utilise les données à caractère personnel en dehors de la «sphère privée», par exemple dans le cadre d'activités sociales et culturelles ou financières, elle est alors tenue de respecter la législation en matière de protection des données.

Exemples

- ✓ **Quand le règlement s'applique**

  Une entreprise établie dans l'UE propose des services de voyage à des clients provenant des États baltes. À cette fin, elle traite les données à caractère personnel de personnes physiques.

- ✓ **Quand le règlement ne s'applique pas**

  Une personne utilise son carnet d'adresses privé pour inviter par e-mail des amis à une soirée qu'elle organise (exception domestique).

.

Quelles sont les données à caractère personnel ?

Les données à caractère personnel sont des informations se rapportant à une **personne vivante identifiée ou identifiable**. Différentes informations, dont le regroupement permet d'identifier une personne en particulier, constituent également des données à caractère personnel.

Des données à caractère personnel qui ont été rendues **anonymes, chiffrées** ou retranscrites sous un **pseudonyme**, mais qui peuvent être utilisées pour identifier à nouveau une personne constituent toujours des données à caractère personnel et sont couvertes par le RGPD.

Les données à caractère personnel rendues **anonymes** de telle manière que la personne ne soit pas ou plus identifiable ne constituent plus des données à caractère personnel. Pour qu'une donnée soit véritablement rendue anonyme, le processus d'anonymisation doit être irréversible.

Le RGPD protège les données à caractère personnel **indépendamment de la technologie utilisée pour le traitement de ces données** – elle est «neutre sur le plan technologique» et s'applique au traitement automatisé et manuel, à condition que les données soient organisées selon certains critères prédéterminés (par exemple: ordre alphabétique). La législation protège également les données indépendamment de la méthode utilisée pour les conserver – dans un système informatique, au moyen de la surveillance vidéo, ou sur papier. Dans tous les cas, les données à caractère personnel sont soumises aux exigences en matière de protection énoncées dans le RGPD.

Exemples

- un prénom et un nom;
- une adresse personnelle;
- une adresse e-mail telle que prénom.nom@entreprise.com;
- un numéro de carte d'identité;
- des données de localisation (par exemple: la fonction de localisation d'un téléphone portable)*;
- une adresse de protocole internet (IP);
- un cookie*;
- l'identifiant publicitaire de votre téléphone;
- des données détenues par un hôpital ou un médecin, qui permettraient d'identifier de manière unique une personne.

**Notez que, dans certains cas, une législation sectorielle spécifique s'applique et réglemente, par exemple, l'utilisation des données de localisation ou des cookies –*

Que recouvre le traitement des données ?

Le «traitement» couvre une large gamme d'opérations effectuées sur des données à caractère personnel, de manière automatisée ou manuelle. Il comprend **la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion** ou toute autre forme de mise à disposition, **le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction** des données à caractère personnel.

Le règlement général sur la protection des données (RGPD) s'applique au traitement automatisé en tout ou en partie, et au traitement non automatisé des données à caractère personnel, si elles figurent dans un fichier structuré.
Exemples de traitement:

- gestion du personnel et administration des salaires;
- accès à/consultation d'une base de données de contacts contenant des données à caractère personnel;
- envoi d'e-mails promotionnels*;
- déchiquetage de documents contenant des données à caractère personnel;
- publication/affichage d'une photo d'une personne sur un site internet;
- conservation d'adresses IP ou d'adresses MAC;
- enregistrement de vidéosurveillance.

Quel est le rôle de l'Autorité de Protection des Données (A.P.D.) ?

Un des rôles de l'APD est de **publier des conseils d'experts** sur les questions relatives à la protection des données.

Elle informe le public sur les droits et obligations liés à la protection des données et, plus particulièrement, sur le règlement général sur la protection des données (RGPD).

Un bon exemple en est l'obligation de l'APD d'établir et de publier une liste des opérations de traitement qui nécessitent une analyse d'impact relative à la protection des données (AIPD protection des données.

L'APD ne peut toutefois pas fournir de conseils dans les cas d'espèce ni remplacer un avocat compétent.

Une administration publique **ne doit pas notifier l'APD qu'elle traite des données.**

Toutefois, **une consultation préalable** avec l'APD est nécessaire lorsque le Délégué à la Protection des Données (DPD) indique que le traitement des données poserait un **risque élevé** et que des risques résiduels persisteraient malgré la mise en œuvre de plusieurs garanties.

En outre, au cas où des données à caractère personnel détenues seraient divulguées de manière accidentelle ou illicite à des destinataires non autorisés, ou si elles étaient temporairement inaccessibles ou altérées, une Administration publique **devrait également contacter l'APD car il s'agirait alors d'un cas de violations de données**.

Une telle violation doit être notifiée à l'autorité de protection des données (APD) dans les meilleurs délais et au plus tard 72 heures après avoir pris connaissance de la violation. L'administration publique pourrait également devoir informer les personnes concernées de la violation

Pour la France, c'est la **CNIL** qui remplit, au plan national, ce rôle d'APD

Quid des administrations publiques ?

Une administration publique est soumise aux règles du RGPD lorsqu'elle traite d**es données à caractère personnel concernant une personne**. Il incombe aux administrations nationales de soutenir les administrations régionales et locales dans la préparation de l'application du RGPD.

En général, les données à caractère personnel détenues par les administrations publiques sont traitées sur la base d'une obligation légale ou dans la mesure où elles sont nécessaires à l'exécution des missions d'intérêt public ou à l'exercice de l'autorité publique dont les administrations sont investies.

Quand elle traite des données à caractère personnel, une administration publique doit s'assurer de respecter des **principes fondamentaux** tels que:

- le traitement loyal et licite;
- la limitation des finalités;
- la minimisation et la conservation des données.

Dans le cas du traitement fondé sur la loi, cette loi devrait déjà garantir le respect de ces principes (par exemple, les types de données, la durée de conservation et les garanties appropriées).

Avant le traitement des données à caractère personnel, **les personnes concernées doivent être informées du traitement, notamment de ses finalités, des types de données collectées, des destinataires, et des droits de ces personnes à la protection des données.**

Le Délégué à la Protection des Données (D.P.D.)

Une administration publique doit **nommer un délégué à la protection des données (DPD).**

Cependant, un seul délégué à la protection des données peut être désigné pour plusieurs organismes publics, et donc être commun à ces organismes.

La sécurisation des données

La collectivité concernée doit également s'assurer d'avoir mis en œuvre les mesures techniques et organisationnelles appropriées pour **sécuriser les données à caractère personnel.** Si des parties du traitement sont sous-traitées à une organisation extérieure (dénommée «sous-traitant»), un contrat ou un autre acte juridique doit être conclu qui **certifie que le sous-traitant fournit les garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées qui respectent les normes du RGPD.**

Le traitement des demandes formulées par les personnes

Des personnes peuvent contacter une administration publique pour exercer leurs droits en vertu du RGPD (**droits d'accès, de rectification, d'effacement, de limitation, d'objection, de ne pas faire l'objet d'une prise de décision automatisée**).

Les personnes concernées ont le **droit de s'opposer** au traitement de leurs données à caractère personnel par l'administration publique pour des missions d'intérêt public.

Elles **doivent communiquer à l'administration publique les raisons liées à leur situation particulière**.

L'administration publique peut continuer à traiter les données, et donc ne pas donner suite à leur demande, si elle démontre qu'elle respecte des motifs légitimes qui prévalent sur les intérêts et les droits de la personne concernée, ou si les données sont nécessaires pour la constatation, l'exercice ou la défense d'un droit en justice.

Les personnes concernées n'ont pas le droit de transmettre de données les concernant qui sont nécessaires à l'exécution d'une mission d'intérêt public ou qui relèvent de l'exercice d'une autorité publique dont elles sont investies.

Une administration publique doit **répondre** aux demandes des personnes dans les meilleurs délais et, en principe, dans un délai d'**un mois** à compter de la réception de la demande.

Elle peut demander des informations supplémentaires pour pouvoir confirmer l'identité de la personne présentant la demande. Si la demande est rejetée, les personnes concernées doivent être informées des raisons de ce rejet et de leur droit à introduire une réclamation auprès de l'APD et à former un recours juridictionnel.

Quelles sont les sanctions applicables en cas de manquement

30 millions d'euros : c'est là l'amende maximale prévue par les textes en cas de manquement à leur obligations légales pour les administrations publiques (ou 4% du chiffre d'affaires mondial pour une entreprise)

6 Étapes recommandées par la CNIL

Étape 1 : Désigner un pilote

C'est le **Délégué à la Protection des Données (DPD)** qui remplit ce rôle (qu'il soit désigné en interne ou mutualiser au niveau supracommunal)

Il exerce une mission d'information, de conseil et de contrôle en interne.

Étape 2 : Cartographier

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par **recenser de façon précise vos traitements de données personnelles**.

L'élaboration d'un **registre des traitements** vous permet de faire le point.

Étape 3 : Dégager des priorités

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir.

Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

Étape 4 : Gérer les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une **analyse d'impact sur la protection des données (AIPD**).

Étape 5 : Organiser les processus internes

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des **procédures internes qui garantissent la prise en compte de la protection des données** à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

Étape 6 : Enregistrer la conformité

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire.

Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Pour toute documentation complémentaire :

CNIL.

www.cnil.fr