



Protection des données : comment se préparer ?

COMPRENDRE LE REGLEMENT GENERAL POUR LA PROTECTION DES DONNEES (RGPD)

1/ DATE D'ENTREE EN VIGUEUR : 25 MAI 2018.

2/ BUTS DU RGPD :

- a) Adapter le droit relatif à la protection des données au développement du numérique;
- b) Harmoniser le dispositif juridique retenu grâce à un texte unique (le RGPD) directement applicable dans toute l'Union européenne.

3/ DIFFERENCES AVEC LE REGIME ANTERIEUR,

- a) Jusqu'alors : obligation de déclaration à la CNIL de vos différents fichiers (clients, prospects, salariés, etc.); et parallèlement : information de ces intéressés, de leur droit d'accès, de rectification ou de suppression de leurs données.
- b) A PARTIR DU 25 MAI : Suppression des formalités indiquées au a) et donc du régime déclaratif

4/ EN QUOI CONSISTE LE REGISTRE DES TRAITEMENTS DES DONNEES PERSONNELLES,

- C'est un fichier électronique – de préférence – ou même éventuellement sous forme «papier» - dans lequel les entreprises doivent faire figurer tous leurs traitements de données personnelles;
- Ce fichier doit, en permanence, être tenu à la disposition de la CNIL (Commission nationale de l'informatique et des libertés).
- En effet, chaque acteur doit, à tout moment, être en mesure de démontrer la conformité de ses activités de traitement à la réglementation applicable.

5/ QU'EST-CE QU'UNE DONNEE PERSONNELLE ?

✓ Est 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.

Exemples : nom, téléphone, date de naissance, adresse, empreinte digitale, numéro d'identification, identifiant en ligne, etc...

✓ Pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc...

6/ QU'EST-CE QU'UN TRAITEMENT DES DONNEES PERSONNELLES ?

a) Opérations concernées :

✓ Il s'agit de toute opération ou ensemble d'opérations impliquant l'utilisation de données personnelles et qui y sont appliquées :

Exemples d'opérations sur des données : 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 mise à disposition, le

rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction des données à caractère personnel.

✓ Donc, toutes les opérations possibles sur des données personnelles sont concernées par le RGPD

b) Exemples de traitement :

- gestion du personnel, administration des salaires ;
- accès à/ou consultation (d')une base de données de contacts contenant des données à caractère personnel;
- envoi d'e-mails promotionnels ;
- destruction 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.

Un registre bien tenu permettra d'avoir une vue d'ensemble des traitements et de pouvoir constater immédiatement les manquements au respect du RGPD.

7/ QUI EST CONCERNE PAR LA TENUE D'UN REGISTRE DE TRAITEMENT DES DONNEES ?

- a) Toutes les entreprises et administrations qui emploient plus de 250 personnes ;
- b) Celles de moins de 250 personnes n'y sont tenues que si leurs traitements portent sur des données sensibles (condamnations, infractions, etc.).

MAIS

La tenue d'un registre est, en pratique, indispensable pour toute entreprise car elle lui permet de prouver à tout moment sa conformité au RGPD. Ceci remplace l'ancienne déclaration obligatoire à la CNIL.

ATTENTION : cette obligation concerne aussi bien les responsables du traitement que les sous-traitants.

8/ A QUI CE REGISTRE PEUT-IL ETRE COMMUNIQUE ?

✓ Evidemment à la CNIL quand elle en fait la demande ;

✓ A tout tiers qui en fait la demande, la transparence étant le principe sur lequel il repose.

9/ CONTENU d'UN REGISTRE ?

✓ Le RGPD ne dresse pas de liste exhaustive des informations devant obligatoirement figurer sur un registre.

✓ Néanmoins, pour être exploitable, il doit obligatoirement contenir les mentions suivantes :

- L'identité et les coordonnées de l'entité concernée (O.P., entreprise ou autre);
- Le nom du responsable du traitement ou de son représentant ; le nom du DPO (Délégué à la protection des données) si l'on en nomme un;
- Les finalités du traitement (Gestion des clients, des recrutements, enquête de satisfaction, vidéo-surveillance, etc.) ;
- Les différentes catégories de données traitées (nom, prénom, téléphone, adresse, données bancaires, habitudes de consommation ...) ;
- Les personnes concernées par le traitement (clients, salariés, fournisseurs, prospects) ;
- Les destinataires des données (vos salariés, vos prestataires, autorités, partenaires) ;
- Les délais prévus de destruction des données et donc la durée de conservation des données ;
- Enumérer et décrire les mesures de sécurité mises en œuvre, pour protéger les données (Confidentialité, chiffrement, anonymisation, pseudonymisation, sécurisation des postes de travail, etc.).

10/ EXISTE-T-IL UN MODELE DE REGISTRE ?

✓ Oui : sur le site de la CNIL, en version EXCEL.

<https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles>

(Modèle de registre règlement européen ; Exemple de fiche de registre CIL [correspondant informatique et liberté]; Règlement européen sur la protection des données personnelles: se préparer en 6 étapes).

11/ RGPD : COMMENT SE PREPARER EN 6 ETAPES ?

- Désigner un pilote :

→ Obligatoire si vous traitez des données à grande échelle ;

→ Utile dans les autres cas de figure car il sera la référence et l'assistant, quant au respect du RGPD de votre entreprise ;

- Cartographier vos traitements de données personnelles :

→ Il s'agit de recenser précisément les traitements des données personnelles que l'on met en œuvre ;

- Prioriser les actions :

→ Sur la base du registre des traitements, il s'agit d'identifier les actions à mener pour être en conformité avec le RGPD (ex. : ne recueillir que les données nécessaires à la réalisation de vos objectifs, vérifier que les sous-traitants connaissent leurs nouvelles obligations, vérifier le droit d'accès des personnes concernées à leurs données...) ;

- Gérer les risques :

→ Il s'agit de mesurer l'impact d'un traitement de données sur la vie privée des intéressés ;

- Organiser les processus internes :

→ Il s'agit de mettre en place des procédures internes qui garantissent à tout moment la protection des données c'est-à-dire au cours de la vie d'un traitement (Ex. : faille dans la sécurité, changement de prestataire, ...) ;

- Documenter la conformité :

→ Afin d'être en mesure de prouver que vous êtes en conformité avec le RGPD, il faut constituer un dossier documentaire, facile à consulter et à vérifier (Ex. : modèles de recueil du consentement des personnes concernées, contrats avec les sous-traitants...)

https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf

Source : CAPEB