Image not found or type unknown

Présentation succincte du RGPD (Règlement Général sur la Protection des Données)

publié le **26/06/2018**, vu **2933 fois**, Auteur : Avocat David MICHEL

Présentation succincte des principes du RGPD (entrée en vigueur 25 mai 2018)

SYNTHESE SUR LE RGPD (APPLICATION AU 25 MAI 2018)

Le 25 mai 2018, entre en application le nouveau Règlement Européen sur la Protection des Données (UE) 2016/679 du 27 avril 2016, dit Règlement Général sur la Protection des Données ou ci-après « RGPD », directement applicable en droit français.

Si le RGPD reprend dans son ensemble les grands principes régissant la protection des données à caractère personnel pour les préciser, il a également pour objet d'introduire de nouvelles obligations pesant sur les responsables de traitement des données dans les entreprises et d'assortir lesdites obligations d'éventuelles sanctions.

Aussi, les entreprises doivent-elles prendre les mesures nécessaires pour examiner leurs processus et systèmes de traitement des différentes données qu'elles sont amenées à collecter et s'assurer de leur conformité au regard du RGPD.

Il est essentiel de rappeler qu'entrent dans le champ d'application non seulement les données dites externes (prospects, clients, fournisseurs..) mais également les données détenues par les entreprises sur leurs salariés.

Aussi, au vu des enjeux et des conséquences pour les sociétés, notamment au regard de la protection des données de leurs propres salariés, cette note aura pour objet de présenter succinctement les points essentiels de cette réforme, en prenant des exemples en matière sociale et de ressources humaines.

1. **DEFINITION DES DONNEES PERSONNELLES**

L'article 4 du RGPD définit la donnée personnelle comme étant toute information se rapportant à une personne physique identifiée ou identifiable par un nom, un numéro d'identification, des données de localisation, un identifiant en ligne...

Cette définition est similaire à celle de la loi n° 78-17 du 6 janvier 1978 dite Loi Informatique et Libertés.

Par exemple, en matière de ressources humaines, doivent notamment être considérées comme des données à caractère personnel :

-

les données collectées lors du recrutement du salarié (les éléments relatifs à son identité et aux ayants droit, son numéro de compte bancaire, son numéro de sécurité sociale, les informations données par le salarié sur les réseaux sociaux tels que Facebook ou Linkedin…)
- les résultats d'examen de la médecine du travail ;
- les données paie ;
- le détail des factures de téléphonie mobile ;
- les courriers électroniques ;
- les logs de connexion du salarié ;
- les horaires des pointeuses, etc…

2. LES PRINCIPES ACTUELLEMENT EN VIGUEUR ET REAFFIRMES PAR LE RGPD

Le RGPD réaffirme des principes essentiels déjà en vigueur, qui ont été notamment retranscrits dans le droit français par la loi dite Informatique et Libertés de 1978.

Ainsi, le traitement des données doit répondre *a minima* aux principes de base posés par l'article 6 de l'actuelle loi Informatique et Libertés, ces principes figurant également à l'article 5 du RGPD.

Selon ces dispositions, ne peuvent faire l'objet d'un traitement que les données :

- collectées et traitées de manière licite et loyale ;
- collectées pour des finalités déterminées, explicites et légitimes, et ne devant pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ;
- exactes, complètes et, si nécessaire, mises à jour ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont collectées et traitées.

3. LES NOUVELLES OBLIGATIONS PESANT SUR LE RESPONSABLE DE TRAITEMENT

Le RGPD supprime la plupart des obligations déclaratives auprès de l'autorité de contrôle à compter du 25 mai prochain étant rappelé qu'en France la mise en place d'un système de traitement de données présuppose actuellement une notification préalable auprès de la CNIL.

En contrepartie, le RGPD accentue les obligations incombant au responsable des traitements de données et aux sous-traitants, qui devront mettre en place les mesures adéquates de protections des données et pouvoir le démontrer, en cas de contrôle, par une documentation adéquate.

Parmi les mesures concrètes à mettre en œuvre par le responsable de traitement et éventuellement, le sous-traitant, le RGPD mentionne :

- la tenue d'un registre des activités de traitement (article 30) ;
- le renforcement des mesures organisationnelles et techniques appropriées afin de garantir un niveau de sécurité adapté au niveau de risque (article 32) ;
- l'obligation de notifier à l'autorité de contrôle (i.e. la CNIL) toute violation de données à caractère personnel (article 33) ;
- l'obligation de communiquer à la personne concernée toute violation de ses données (article 34) ;

Copyright © 2025 Légavox.fr - Tous droits réservés

- le cas échéant, la réalisation d'une étude d'impact relative à la protection des données (article 35) ;
- la désignation d'un délégué à la protection des données dans certains cas (article 37) (cf paragraphe 5 ci-après).

4. **LE RENFORCEMENT DU DROIT DES PERSONNES CONCERNEES PAR LE TRAITEMENT DES DONNEES PERSONNELLES**

Le RGPD renforce le droit des personnes concernées par le traitement des données personnelles, notamment :

- en prévoyant un droit à l'information renforcé par la mise à disposition d'une information claire, intelligible et aisément accessible et par l'obtention du consentement des personnes concernées, un consentement tacite n'étant plus accepté ;

- en consacrant un droit à l'oubli, c'est-à-dire en leur octroyant un droit d'obtenir du responsable du traitement, dans les meilleurs délais, l'effacement des données à caractère personnel les concernant ;

- en créant un droit à la portabilité des données de nature à permettre aux personnes concernées d'exiger des responsables de traitement la transmission de leurs données à caractère personnel à un autre responsable de traitement, sans que le responsable de traitement ayant initialement collecté les données puissent s'y opposer.

5. **LE DELEGUE DES DONNEES PERSONNELLES OU DPD**

Le RGPD prévoit également la désignation d'un délégué à la protection des données (DPD), qui est obligatoire dans certains cas (organismes publics, organismes traitant à grande échelle des données sensibles ou de façon régulière et systématique) et fortement recommandée dans les autres cas (articles 37 et suivants du RGPD).

Le DPD, désigné sur la base de ses qualifications, a pour rôle d'être l'interlocuteur privilégié quant à l'application du RGPD dans la structure, dans la mesure où il est à la fois chargé d'informer le responsable du traitement des données (ou le sous-traitant) et/ou les employés en charge du traitement, de contrôler le respect du RGPD au sein de l'établissement et d'être le point de contact avec l'autorité de contrôle (i.e. la CNIL).

Le DPD bénéficie d'un statut particulier développé à l'article 38 du RGPD : indépendance et absence d'instructions quant à l'exercice de ses missions, octroi des ressources nécessaires pour exercer sa mission, impossibilité d'être relevé de ses fonctions ou pénalisé par le responsable du traitement, absence de conflits d'intérêts en cas d'exercice d'autres missions et tâches au sein de la structure.

Ainsi, le DPD dispose d'un statut spécifique, en étant à la fois indépendant tout en étant potentiellement salarié de l'organisme concerné et proche de la Direction sans pour autant être en conflit d'intérêt et en n'étant pas considéré comme un salarié protégé au sens du droit du travail…

6. **LES SANCTIONS EN CAS DE MANQUEMENT**

Le RGPD a accru le pouvoir de sanction des autorités de contrôle nationales, à savoir la CNIL en France.

Copyright © 2025 Légavox.fr - Tous droits réservés

Outre le pouvoir d'imposer des mesures correctives (avertissement, interdiction du traitement…), l'autorité de contrôle pourra désormais sanctionner d'une amende administrative pouvant atteindre 10.000.000 € ou 2% du chiffre d'affaires mondial de l'exercice précédent, le montant le plus élevé étant appliqué.

En cas de violations plus graves, affectant par exemple la licéité du traitement, le recueil du consentement, les droits des personnes tels que le droit d'accès, de rectification, d'effacement…, les sanctions sont susceptibles d'atteindre jusqu'à 20.000.000 € ou 4% du chiffre d'affaires mondial de l'exercice précédent.

De surcroît, tout manquement à la législation en la matière pourra donner lieu à une action en réparation du préjudice subi par les personnes concernées ou à des sanctions pénales (peine d'emprisonnement de cinq ans et amende de 300.000 euros, multipliée par cinq pour les personnes morales, conformément aux articles 226-16 à 226-24 du Code Pénal).

L'on rappellera également que selon une jurisprudence constante, la preuve de faits obtenus par un dispositif de traitement de données personnelles non conforme est inopposable. Ainsi, en matière de droit du travail, un dispositif non conforme et illicite ne peut servir de preuve à l'appui d'un licenciement (Voir, par exemple, un arrêt de la Cour de Cassation de 2014, qui rejette la recevabilité des informations collectées par un système de traitement automatisé avant sa déclaration à la CNIL, qui avaient été utilisées par l'employeur pour prouver le grief invoqué, à savoir, en l'espèce, une utilisation excessive par la salariée de sa messagerie électronique à des fins personnelles (Cass. soc., 08 octobre 2014, n° 13-14991)).

Enfin, au-delà de ces sanctions pécuniaires et au vu du contexte actuel dans lequel s'inscrit le RGPD (scandale Facebook-Cambridge Analytica…), une éventuelle violation des règles applicables en matière de protection de données personnelles pourrait être de nature à mettre en jeu la réputation des entreprises fautives et la confiance qui leur est accordée.

EN CONCLUSION

Au vu des obligations mises à la charge des entreprises et des éventuels risques et sanctions, il est important pour les entreprises de s'assurer, dans les meilleurs délais, de la mise en conformité de leur traitement des différentes données personnelles (clients, fournisseurs, salariés…), qu'elles sont amenées à collecter avec les nouvelles dispositions qui sont en vigueur à compter du 25 mai 2018.

Je reste à votre disposition pour vous apporter de plus amples précisions et/ou vous assister et accompagner si besoin dans la mise en œuvre de cette réforme**.**

Avertissement : Les informations contenues dans cet article ne sont livrées qu'à titre purement informatif. Elles ne constituent en aucune façon une consultation ou un conseil. Le lecteur ne doit en aucune circonstance agir ou ne pas agir sur la base des informations disponibles dans cet article sans rechercher le conseil préalable d'un professionnel du droit donné en fonction des circonstances propres à chaque affaire.

--

David MICHEL

Avocat au Barreau de Paris

Copyright © 2025 Légavox.fr - Tous droits réservés

5 rue Jules Lefebvre 75009 Paris

Toque K0056

davidmichel.avocat@gmail.com

06.17.41.78.53

Copyright © 2025 Légavox.fr - Tous droits réservés