Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA ZONE DE DÉFENSE ET DE SÉCURITÉ EST

Direction régionale de l'alimentation, de l'agriculture et de la forêt

25 mai 2018

Le règlement général sur la protection des données (RGPD)

Au même titre que d'autres secteurs d'activité, les entreprises des **secteurs agricoles et agro-alimentaires** sont susceptibles d'être concernées par différents enjeux de sécurité économique. La présente fiche poursuit un objectif de relais de sensibilisation sur le règlement général sur la protection des données (RGPD). Elle ne préjuge pas des informations plus détaillées par ailleurs accessibles selon d'autres canaux.

✓ Le RGPD, de quoi s'agit-il ?

Le règlement 2016/679 du 27 avril 2016, dit règlement général sur la protection des données (RGPD), est le nouveau cadre réglementaire européen pour le traitement et la circulation des données à caractère personnel.

Le RGPD se substitue à la directive 95/46/CE du 24 octobre 1995. Il s'applique directement dans tous les États membres depuis le **25 mai 2018**.

Les objectifs du RGPD sont de :
- renforcer et unifier les droits des résidents européens dont les données personnelles pourraient être traitées ;
- responsabiliser les acteurs traitant ces données ;
- instaurer de nouveaux droits pour les résidents européens : droit de consentement (accord explicite sur le traitement des données), droit d'information (sur la finalité des traitements, sur la violation éventuelle des données,…), droit de portabilité (récupération des données), droit à l'oubli (effacement des données), etc.

✓ Qui est concerné ?

Tout acteur traitant des données à caractère personnel :
- le **responsable du traitement**, c'est-à-dire la personne physique ou morale, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens de du traitement,
- mais également ses **sous-traitants éventuels**.

✓ Donnée à caractère personnel

Une donnée à caractère personnel, ou donnée personnelle, est une information qui permet d'identifier une personne physique, directement ou indirectement.

Le champ en est très étendu : il peut s'agir d'un nom, d'une photographie, d'une date de naissance, d'un numéro de téléphone, d'une adresse postale, d'une adresse IP, d'une empreinte digitale, d'un numéro d'immatriculation, d'un enregistrement vocal, d'un numéro de sécurité sociale, etc.

Parmi les données personnelles, sont dites sensibles celles d'entre elles qui font apparaître les origines raciales ou ethniques, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le données génétiques, biométriques, liées à la santé, à la vie ou à l'orientation sexuelles. Les données sensibles font l'objet d'une interdiction générale de collecte et de traitement, sauf exceptions limitatives.

✓ Traitement de données

Au sens du RGPD, constitue un traitement de données toute opération ou ensemble d'opérations, automatisées ou non, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la communication par transmission ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la destruction,…, des données concernées.

✓ Obligations générales liées au règlement

Le traitement des données doit s'inscrire dans un **ensemble de limites** visant à ne pas porter atteinte aux droits et libertés des personnes :
- les données doivent être collectées pour des finalités déterminées, explicites et légitimes ;
- elles doivent être adéquates, pertinentes et non excessives au regard des finalités du traitement ;
- elles doivent être traitées de manière sécurisée, notamment afin d'empêcher qu'elles ne soient déformées, endommagées ou que des tiers non autorisés y aient accès ;
- elles ne peuvent être conservées que pendant une durée déterminée, justifiée par la finalité du traitement.

Le règlement introduit d'autres obligations, dont les plus significatives sont les suivantes.

Avant le RGPD, le responsable du traitement devait réaliser des formalités préalables (déclaration ou autorisation) auprès de la commission nationale informatique et libertés (CNIL). Le RGPD y substitue un **principe de responsabilité** : il appartient désormais au responsable du traitement de mettre en place des procédures internes lui permettant de garantir et de justifier du respect des règles de protection des données personnelles.

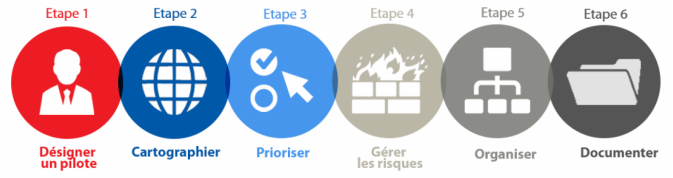
Le règlement pose également les obligations de protection des données **dès la conception et par défaut**.

Il prévoit enfin que le responsable du traitement doit informer la CNIL et la personne physique concernée, en cas de risque élevé pour ses droits et libertés, de toute **violation des données personnelles**. La notification à la CNIL doit alors intervenir dans les délais les plus rapides et, si possible, 72 heures au plus tard après en avoir pris connaissance.

✓ Comment intégrer les obligations du RGPD ?

Pour se mettre en conformité avec le règlement, la CNIL propose une méthodologie en six étapes :

1. **désigner un pilote de la gouvernance des données personnelles** au sein de la structure, le délégué à la protection des données ;
2. **cartographier ses traitements de données personnelles** ; l'élaboration d'un registre des traitements permet de faire le point ;
3. **identifier les actions à mener** pour se conformer aux obligations **et les prioriser** selon les risques que les traitements font peser sur les droits et libertés des personnes ;
4. **produire**, si des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes sont identifiés, **une analyse d'impact** sur la protection des données (PIA) ;



Les 6 étapes pour intégrer le RGPD *(source : CNIL)*

5. **mettre en place des procédures internes** qui assurent 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 ;
6. **constituer une documentation** permettant de justifier d'une protection des données en continu.

Au cas par cas, **le contenu exact et le niveau d'approfondissement des mesures à prendre pourront varier assez fortement** selon le niveau de risque lié aux données, mais également selon la taille de l'entreprise, son modèle économique,..., paramètres en fonction desquels le patrimoine de données sera plus ou moins étendu.

✓ Contrôles et sanctions

En France, la CNIL est l'autorité compétente pour la protection des données personnelles.

Elle dispose d'un pouvoir de contrôle et de sanctions envers les responsables de traitement. Elle peut rendre publiques les sanctions pécuniaires qu'elle prononce.

Après le 25 mai, tout traitement en infraction avec le RGPD pourrait être sanctionné par une amende pouvant aller jusqu'à **20 millions d'euros** ou, dans le cas d'une entreprise, **4% de son chiffre d'affaires annuel mondial total**.

✓ Bénéfices à retirer du RGPD

Le RGPD ne se réduit pas à des obligations…

Le nouveau cadre réglementaire a vocation à **procurer des avantages** aux citoyens, aux entreprises, aux administrations,..., du fait de traitements qui présentent des garanties renforcées pour la protection des données personnelles.

Pour une entreprise, le RGPD donne l'opportunité :

- d'avoir une réflexion structurante sur les moyens à mobiliser pour une mise en conformité proactive, fondée sur la responsabilité ;
- de « mettre de l'ordre » dans la gestion de ses données à caractère personnel, d'acquérir une connaissance renforcée des données détenues et du potentiel de valorisation qu'elles peuvent présenter ;
- de construire une relation plus forte avec ses clients, fondée sur la transparence et la confiance.

Les entreprises peuvent ainsi envisager de tirer profit du règlement pour conforter la confiance, améliorer leur image,..., en tirer des avantages compétitifs.

✓ Outils et liens utiles

Afin d'accompagner les acteurs concernés, la CNIL met à disposition différents outils, parmi lesquels :

- un **guide de la sécurité des données personnelles** en 17 fiches : https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
- un **modèle de registre de traitement des données** : https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles
- le **logiciel open source PIA**, destiné à faciliter la conduite et la formalisation d'analyses d'impact sur la protection des données : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
- une **foire aux questions** visant à orienter au mieux les professionnels et le public : https://www.cnil.fr/fr/cnil-direct/thematique/143?visiteur=pro

Compte tenu de la difficulté particulière que la mise en conformité avec le RGPD pourrait poser aux petites et moyennes entreprises, la CNIL a par ailleurs élaboré, en partenariat avec la banque publique d'investissement, un guide spécialement conçu, le **« Pack TPE-PME »** : https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement

---

Contact DRAAF :

Mission défense et sécurité de zone Est
Mél : jean-francois.laigre@agriculture.gouv.fr
Tél : 03 55 74 10 82