Obligations en matière de protection des données personnelles

Vérifié le 03 avril 2019 - Direction de l'information légale et administrative (Premier ministre), Ministère chargé de la justice

La création et le traitement de données personnelles (numéro d'identifiant, nom, adresse, numéro de téléphone, photo, adresse IP notamment) sont soumis à des obligations destinées à protéger la vie privée et les libertés individuelles. De nouvelles obligations sont à la charge des entreprises, administrations, collectivités, associations ou autres organismes permettant d'accorder des droits plus étendus à leurs clients / usagers. Le régime des sanctions évolue également.

Qu'est-ce qu'une donnée personnelle ?

Il s'agit de toutes informations se rapportant à une personne physique identifiée ou identifiable, directement ou non, grâce à un identifiant ou à un ou plusieurs éléments propres à son identité.

Il peut s'agir par exemple d'un nom, d'un prénom, d'une adresse électronique, d'une localisation, d'un numéro de carte d'identité, d'une adresse IP, d'une photo, d'un profil social ou culturel.

Les règles s'appliquent lorsqu'elles sont utilisées, conservées ou collectées numériquement ou sur papier.

Qui est concerné ?

Le règlement s'applique à tous les traitements de données à caractère personnel, sauf exceptions (les fichiers de sécurité restent régis par les États et les traitements en matière pénale par exemple).

Il concerne :

- les responsables de traitement (entreprises, administrations, associations ou autres organismes) et leurs sous-traitants (hébergeurs, intégrateurs de logiciels, agences de communication entre autres) établis dans l'Union européenne (UE), quel que soit le lieu de traitement des données.
- les responsables de traitement et leurs sous-traitants établis hors de l'UE, quand ils mettent en œuvre des traitements visant à fournir des biens ou des services à des résidents européens ou lorsqu'ils les ciblent avec des techniques algorithmiques (technique du profilage).

En pratique, le règlement s'applique donc à chaque fois qu'un résident européen, quelle que soit sa nationalité, est directement visé par un traitement de données, y compris par internet ou par le biais d'objets connectés (appareils domotiques, objets mesurant l'activité physique par exemple).

Droit des personnes

Consentement renforcé et transparence

Les données personnelles doivent être :

- traitées de manière licite, loyale et transparente et collectées pour des finalités déterminées ;
- explicites et légitimes ;
- adéquates, pertinentes et limitées aux finalités du traitement ;
- exactes et tenues à jour ;
- conservées de façon temporaire et sécurisée.

Les clients ont un droit d'accès à leurs données et peuvent les rectifier et s'opposer à leur utilisation.

Sur demande, l'entreprise qui détient des données personnelles doit informer la personne concernée avec les éléments suivants :

- identité du responsable du fichier ;
- finalité du traitement des données ;
- caractère obligatoire ou facultatif des réponses ;
- droits d'accès, de rectification, d'interrogation et d'opposition ;
- les obligations induites par les transmissions des données.

Droit à la portabilité des données

Toute personne peut récupérer, sous une forme réutilisable, les données qu'elle a fournies et les transférer ensuite à un tiers (réseau social par exemple).

La portabilité concerne uniquement les données recueillies dans le cadre d'un contrat ou d'un consentement.

Droit à l'oubli

Toute personne a droit à l'effacement de ses données et au déréférencement (droit de demander à un moteur de recherche de supprimer certains résultats associés à ses noms et prénoms).

Droit à notification

En cas de violation de la sécurité des données comportant un risque élevé pour les personnes, le responsable du traitement doit les avertir rapidement, sauf dans certaines situations (données déjà chiffrées par exemple). Il doit également le notifier à la Cnil dans les 72 heures.

Droit à réparation du dommage matériel ou moral

Toute personne qui a subi un dommage matériel ou moral du fait de la violation du règlement européen peut obtenir du responsable du traitement (ou du sous-traitant) la réparation de son préjudice.

Action de groupe

Toute personne peut mandater une association ou un organisme actif dans le domaine de la protection des données pour faire une réclamation ou un recours et obtenir réparation en cas de violation de ses données.

Obligations des entreprises, administrations, collectivités, associations

Obligation générale de sécurité et de confidentialité

Le responsable du traitement des données doit mettre en œuvre les mesures de sécurité des locaux et des systèmes d'information pour empêcher que les fichiers soient déformés, endommagés ou que des tiers non autorisés y aient accès.

Il doit prendre toutes les mesures nécessaires au respect de la protection des données personnelles dès la conception du produit ou du service.

Ainsi, il est tenu de limiter la quantité de données traitée dès le départ (principe dit de « minimisation ») et doit démontrer cette conformité à tout moment.

L'accès aux données est réservé uniquement aux personnes désignées ou à des tiers qui détiennent une autorisation spéciale et ponctuelle (service des impôts par exemple.).

Le responsable des données doit fixer une durée raisonnable de conservation des informations personnelles.

Les obligations déclaratives sont toutes supprimées, sauf exceptions prévues par le droit national (certains traitements dans le secteur de la santé, ou de la sécurité publique mis en œuvre pour le compte de l'État).

Obligation d'information

L'entreprise qui détient des données personnelles doit informer la personne concernée de :

- l'identité du responsable du fichier ;
- la finalité du traitement des données ;
- le caractère obligatoire ou facultatif des réponses ;
- les droits d'accès, de rectification, d'interrogation et d'opposition ;
- les transmissions des données.

L'exploitant de données personnelles (un commerçant en ligne par exemple) doit respecter certaines obligations, et notamment :

- recueillir l'accord des clients ;
- informer les clients de leur droit d'accès, de modification et de suppression des informations collectées ;
- veiller à la sécurité des systèmes d'information ;
- assurer la confidentialité des données ;
- indiquer une durée de conservation des données.

L'objectif de la collecte d'informations doit être précis et les données en accord avec cette finalité.

À savoir : la majorité numérique, l'âge à partir duquel un mineur peut consentir seul au traitement de ses données personnelles pour utiliser un service sur internet (les réseaux sociaux par exemple), est fixée à 15 ans. L'autorisation des parents est nécessaire avant cet âge. L'information relative au traitement de données du mineur doit être rédigée en termes clairs et simples.

Analyse d'impact en cas de risque élevé pour les droits et libertés des personnes

Pour les traitements de données présentant un risque élevé pour les droits et libertés des personnes, le responsable du traitement doit mener une analyse d'impact sur la vie privée (PIA) pour évaluer , en particulier, l'origine, la nature, la particularité et la gravité de ce risque.

Cette étude doit être présentée à laCnil si elle n'a pas permis de diminuer suffisamment le risque pour le rendre acceptable.

Les données concernées doivent porter sur :

- les informations sensibles (origine, opinions politiques, religieuses, syndicales), biométriques ou génétiques notamment ;
- l' évaluation des personnes (profilage par exemple) ;
- les fichiers ayant une finalité particulière (études statistiques de l'Insee, traitements de recherche médicale par exemple) ;
- les transferts de données hors de l'Union européenne.

À noter : les transferts de données hors de l'UE ne sont plus interdits mais ils doivent respecter plusieurs conditions, notamment que le pays tiers présente un niveau de protection adapté, selon la Commission européenne. Une autorisation de la Cnil est nécessaire si des clauses contractuelles diffèrent des clauses de la Commission européenne. Les données transférées restent soumises au droit de l'UE non seulement pour leur transfert, mais aussi pour tout traitement / transfert ultérieur.

Délégué à la protection des données

Le responsable de traitement et le sous-traitant doivent désigner un délégué à la protection des données :

- si leur activité fait partie du secteur public ;
- si leur activité principale amène un suivi régulier et systématique de personnes à grande échelle ;
- si leur activité principale amène le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et infractions.

Le délégué est chargé :

- d'informer et de conseiller le responsable de traitement (ou le sous-traitant) et ses employés ;
- de contrôler le respect du règlement européen et du droit français en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être son contact.

Le délégué à la protection des données doit avoir les qualités et compétences suivantes :

- communiquer efficacement et exercer ses fonctions en toute indépendance (ne pas avoir de de conflit d'intérêts avec ses autres missions) ;
- une expertise en matière de législations et pratiques (protection des données), acquise notamment par une formation continue ;
- une bonne connaissance du secteur d'activité et de l'organisation de l'organisme (opérations de traitement, systèmes d'information et besoins de l'organisme en matière de protection et de sécurité des données) ;
- une position efficace en interne pour faire un rapport au niveau le plus élevé de l'organisme ;
- animer un réseau de relais au sein des filiales d'un groupe par exemple et/ou une équipe d'experts en interne (expert informatique, juriste, expert en communication, traducteur par exemple).

Le délégué peut être une personne issue du domaine technique, juridique ou autre.

Autres obligations

Tous les organismes (publics comme privés) qui traitent des données personnelles ont l'obligation de tenir un registre de l'ensemble des traitements.

Toutefois les entreprises de moins de 250 salariés doivent seulement inscrire au registre :

- les traitements non occasionnels ;
- les traitements susceptibles de comporter un risque pour les droits et libertés des personnes ;
- les traitements qui portent sur des données sensibles.

Sanctions administratives

En cas de violation du règlement, la Cnil peut prononcer des amendes administratives qui peuvent atteindre, selon la catégorie du manquement,2 % à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent.

Textes de référence

- Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679)
- Ordonnance n° 2018-1125 du 12 décembre 2018 sur la protection des données personnelles et modifiant la loi n° 78-17 du 6 janvier 1978 (https://www.legifrance.gouv.fr/eli/ordonnance/2018/12/12/JUSC1829503R/jo/texte)
- Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037085952)
  art.8 (certaines catégories de données : origine/opinion) ; art. 16 (catégorie particulière de traitement : santé)
- Loi n°78-17 du 6 janvier 1978 - Informatique et libertés (http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624)
- Loi n°2016-1321 du 7 octobre 2016 pour une République numérique (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000033205014)
  cles 48 (entrée en vigueur des dispositions relatives à la portabilité des données) et 65 (sanctions prononcées par la Cnil)
- Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037277401)
- Code de la consommation : articles L224-42-1 à L224-42-4 (https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000033206899&cidTexte=LEGITEXT000006069565)
  Récupération et portabilité des données
- Code pénal : articles 226-16 à 226-24 (http://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000006165313&cidTexte=LEGITEXT000006070719)
  Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques
- Décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi de 1978 relative à l'informatique, aux fichiers et aux libertés (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038528420)
- Délibération n° 2018-326 du 11 octobre 2018 sur les lignes directrices des analyses d'impact sur la protection des données (AIPD) (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037559518)
- Délibération n°2018-327 du 11 octobre 2018 sur les types d'opérations de traitement avec analyse d'impact sur la protection des données (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037559521)

Services en ligne et formulaires

- Demande d'autorisation d'un traitement de recherche dans le domaine de la santé (https://www.service-public.fr/professionnels-entreprises/vosdroits/R18457)
  Formulaire
- Demande d'autorisation d'un traitement ayant pour finalité l'évaluation ou l'analyse des pratiques ou des activités de soins et de prévention (https://www.service-public.fr/professionnels-entreprises/vosdroits/R18458)
  Formulaire
- Désignation d'un correspondant Informatique et libertés (CIL) à la protection des données à caractère personnel (https://www.service-public.fr/professionnels-entreprises/vosdroits/R12144)
  Formulaire
- Désignation d'un correspondant Informatique et libertés (CIL) à la protection des données à caractère personnel - Presse (https://www.service-public.fr/professionnels-entreprises/vosdroits/R12283)
  Formulaire
- Demandes en ligne d'autorisation ou d'avis à la Cnil (https://www.service-public.fr/professionnels-entreprises/vosdroits/R1409)

Téléservice

Pour en savoir plus

- RGPD : de quoi s'agit-il ? (https://www.vie-publique.fr/eclairage/19588-rgpd-reglement-general-sur-la-protection-des-donnees-de-quoi-sagit-il)
  Vie-publique.fr
- Infographie : obligations pour votre entreprise (http://ec.europa.eu/justice/smedataprotect/index_fr.htm)
  Commission européenne
- RGPD : se préparer en 6 étapes (https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes)
  Commission nationale de l'informatique et des libertés (Cnil)
- Guide pratique CNIL/BPI France adapté aux TPE/PME (https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement)
  Commission nationale de l'informatique et des libertés (Cnil)
- Outil PIA en téléchargement : faciliter la conduite d'analyses d'impact (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil)
  Commission nationale de l'informatique et des libertés (Cnil)
- Formation en ligne de la CNIL sur le RGPD (https://www.cnil.fr/fr/la-cnil-lance-sa-formation-en-ligne-sur-le-rgpd-ouverte-tous)
  Commission nationale de l'informatique et des libertés (Cnil)
- Règles à respecter pour le contrôle d'accès biométrique sur le lieu de travail (https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail)
  Commission nationale de l'informatique et des libertés (Cnil)
- Le registre des activités de traitement : RGPD (https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement)
  Commission nationale de l'informatique et des libertés (Cnil)