

Encadrer l'exploitation des données numériques

DE QUOI PARLE-T-ON ?

- La notion de données personnelles est définie par l'article 4 du règlement européen n° 2016/679 du 27 avril 2016 de la manière suivante : « toute information se rapportant à une personne physique identifiée ou identifiable (...) ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. »
- Le sigle RGPD signifie « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Regulation » ou GDPR). Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

APPLIQUER LA RÉGLEMENTATION

Les employeurs doivent se conformer au respect du règlement général sur la protection des données personnelles (RGPD) issu du règlement européen n° 2016/679 du 27 avril 2016, d'application directe aux états membres, entré en vigueur le 25 mai 2018.

Il s'agit d'appliquer les cinq règles de base en matière de données numériques (cf schéma fiche 10) :

- La finalité, conduisant à traiter des données personnelles des salariés, doit être clairement défini, dans le respect des dispositions légales et réglementaires.
- Les salariés doivent être informés des traitements de leurs données personnelles et leur consentement éclairé doit être recueilli lorsqu'il est obligatoire.
- Seules les données pertinentes répondant aux objectifs poursuivis doivent être exploitées et leur confidentialité doit être assurée.
- Les durées de conservation des données doivent être déterminées en fonction de leurs caractéristiques et finalités.
- Le droit d'accès et de rectification des données personnelles, le droit à l'effacement des données et leur portabilité le cas échéant doivent être garantis selon les modalités légales et réglementaires.

Il faut veiller à ce que les prestataires ou sous-traitants respectent les règles de protection des données et s'assurer que les innovations et développements futurs des technologies numériques tels que l'Intelligence artificielle et les algorithmes de management respectent le cadre de la protection des données.

Le rôle du DPO (délégué à la protection des données)

- **Missions**
Le délégué est chargé de mettre en conformité avec le règlement européen sur la protection des données (RGPD), les pratiques de collecte et de traitement de l'organisme qui l'a désigné.
- **Obligations**
La désignation d'un délégué est obligatoire pour :
 - Les autorités ou les organismes publics.
 - Les organismes amenés à réaliser un suivi régulier et systématique des personnes à grande échelle.
 - Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.
- **Pour une information actualisée**
www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo
www.cnil.fr/fr/designation-dpo

Gestion du recrutement, de la paie ou des carrières

- **Quelles données peut-on collecter ?**

Les données collectées lors du processus de sélection ne doivent servir qu'à évaluer la capacité du candidat à occuper l'emploi proposé (qualification, expérience, détention du permis de conduire etc.). Lorsque la personne est recrutée, l'entreprise est autorisée à recueillir les données nécessaires à la gestion administrative et sociale du salarié :

Autorisées	Interdites
<ul style="list-style-type: none"> • Informations nécessaires au respect d'une obligation légale (exemple : déclarations sociales obligatoires) • Informations utiles à la gestion administrative du personnel (par exemple, type de permis de conduire détenu ou coordonnées de personnes à prévenir en cas d'urgence) • Informations utiles à l'organisation du travail (par exemple, photographie facultative du salarié pour les annuaires internes et organigrammes) • Informations utiles à l'action sociale prise en charge par l'employeur (par exemple, les informations concernant les ayants-droit du salarié). 	<ul style="list-style-type: none"> • Collecter des informations sur ses parents, sa fratrie, ses opinions politiques ou son appartenance syndicale.

- **La durée de conservation des données est variable selon la situation**

- **L'accès aux données doit être :**

1. Limité aux personnes intervenant dans les processus de recrutement et celles chargées de la gestion du personnel et limité aux informations nécessaires à l'exercice de la fonction (supérieur hiérarchique, délégué du personnel...)
2. Conditionné par un accord préalable dans certains cas
3. Sécurisé par une politique d'habilitation et par le traçage des accès (qui se connecte à quoi, quand et pour faire quoi ?)

- **Le droit à l'information doit être respecté** : vis-à-vis des représentants du personnel et vis-à-vis des candidats et salariés (informations à transmettre obligatoirement et droit de consultation)

- **Zones « bloc note » et « commentaires » : attention à ne pas dérapier**

L'utilisation de zones de commentaires libres (une zone de texte libre dans un formulaire ou une colonne « commentaires » dans un tableur), dite également "zones bloc-notes" est une pratique courante au sein de nombreux organismes. Elle permet par exemple d'assurer le suivi d'un dossier client ou de personnaliser la relation commerciale. Néanmoins, son usage comporte des risques au regard de la vie privée.

La CNIL, qui a déjà sanctionné à plusieurs reprises des dérives, rappelle les réflexes à adopter.

- Règle n° 1 : informer les personnes concernées par la collecte de données personnelles
- Règle n° 2 : penser au droit d'accès
- Règle n° 3 : être objectif, jamais excessif ou insultant

Les informations collectées sur les personnes doivent être adéquates, pertinentes et non excessives au regard de la finalité du traitement envisagé, qu'il soit automatisé ou au format papier. Les commentaires ne doivent pas être inappropriés, subjectifs et insultants.

- **Pour une information actualisée**

www.cnil.fr/fr/travail-et-donnees-personnelles

www.cnil.fr/fr/le-recrutement-et-la-gestion-du-personnel

www.cnil.fr/fr/lacces-son-dossier-professionnel

www.cnil.fr/fr/zones-bloc-note-et-commentaires-les-bons-reflexes-pour-ne-pas-deraper