Données personnelles et gestion des ressources humaines

Foire aux questions

Ce document a été élaboré à partir des questions remontées par les adhérents en 2021 notamment lors du webinaire du 23 novembre 2021 dédié à la protection des données en matière de gestion des ressources humaines lors duquel sont intervenus :

- La FAS pour une présentation des enjeux dans le secteur de l'inclusion sociale ;
- La CNIL pour une présentation de la thématique données personnelles / gestion des ressources humaines ;
- Un adhérent pour un témoignage sur la sécurisation des données dans sa structure.

1. Les relations entre les acteurs de la protection des données

- **Est-ce que l'utilisateur est responsable des données si elles disparaissent ou sont introuvables ?**

Rappel sur la notion de responsable de traitement

Le responsable de traitements est une personne morale qui va mettre en place le traitement de données et définir sa finalité (= objectif poursuivi) et ses moyens (c'est-à-dire ses modalités : base légale, durée de conservation, catégorie de données collectées, mesures de sécurité...). Il faut bien noter que le responsable de traitements ne sera pas l'un de ses dirigeants à titre individuel.

Ce ne sera pas non plus l'un de ses préposés (membre du personnel : salarié, stagiaire, bénévole, intérimaire ...) même s'il est utilisateur d'un outil informatique traitant des données personnelles.

Non, la responsabilité individuelle de l'utilisateur ne sera pas mise en jeu en cas de perte ou vol de données à l'égard de l'autorité de contrôle mais celle du responsable de traitements pourra l'être (ce qui n'empêche pas, s'agissant du salarié, d'encourir des sanctions disciplinaires). Diverses solutions peuvent permettre de prévenir la violation de données et limiter sa responsabilité comme prévoir des mesures de sécurité organisationnelles (ex : sensibilisation des utilisateurs sur les risques de phishing et mise en place d'une procédure destinée à gérer ce risque en interne) et d'autres techniques (gestion des habilitations d'accès, mise en place d'un VPN ...).

2. Le champ d'application du RGPD

- **Les données transformées en statistiques (ex : tranche d'âge des salariés) sont-elles aussi soumises au RGPD ?**

Rappel des notions clés du RGPD : données personnelles et traitement de données

Les règles du RGPD s'appliquent uniquement aux traitements de données dites personnelles, c'est-à-dire celles qui permettent d'identifier une personne physique de manière directe (ex : prénom, nom) ou de manière indirecte (ex : numéro de téléphone). Le traitement fait l'objet lui aussi d'une définition juridique.

Elle est très large car cela se rapporte à toute opération portant sur des données personnelles (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement) qu'elles soient en format numérique ou papier !

Au vu de ce qui précède, seules les données personnelles collectées sont soumises au RGPD. S'agissant de statistiques qui révèlent la tranche d'âge des salariés, on peut envisager deux cas de figure :

- **ces statistiques ne sont pas anonymisées** en ce sens que des données personnelles permettent **d'identifier des salariés directement** (ex : par son nom de famille) ou **indirectement par recoupement** (ex : matricule interne du salarié pouvant être identifié en le recoupant avec les dossiers du personnel)

▶ le RGPD s'applique : il faut donc identifier notamment la finalité, la base légale de ce traitement de données et en informer les salariés.

- **ces statistiques sont anonymisées en ce sens qu'aucun salarié ne peut être identifié** de manière directe ou indirecte ; ce type de catégories de données ayant été effacé des statistiques

▶ le RGPD ne s'applique pas vu que les données sont anonymes.

Point de vigilance : cela n'exonère pas le responsable de traitements d'informer les personnes au moment de la collecte des données personnelles qu'elles serviront ensuite à générer des statistiques anonymes.

Pour plus d'information sur les techniques d'anonymisation proposées par la CNIL : cliquez ici.

3. Les principes encadrant la durée de conservation des données

- **Combien de temps doit-on garder le dossier du personnel et les fiches de paies après le départ du salarié ?**

Rappel des principes encadrant la durée de conservation des données personnelles

Le RGPD prévoit que les données personnelles ne peuvent être collectées que la durée nécessaire à l'accomplissement de la finalité. Une fois la finalité du traitement (c'est à dire l'objectif poursuivi) accomplie, le responsable de traitements pourra les supprimer, les anonymiser ou les archiver. Pour l'archivage, cela implique notamment de cesser de conserver les données « à porter de main » et de limiter l'accès aux données qu'aux personnes habilitées. S'agissant de la possibilité d'archiver les données, le responsable de traitements peut le faire uniquement s'il a un intérêt réel (par exemple, se ménager des preuves en cas de contentieux).

Comment déterminer la durée de conservation et d'archivage (s'il y a un intérêt réel à y procéder) ?

La même méthode s'applique pour les deux.

En premier lieu, il faut rechercher s'il y a un texte légal ou règlementaire qui en prévoit.

C'est souvent le cas s'agissant des traitements RH ; le Référentiel RH de la CNIL recensant les durées souvent prévues par le code du travail.

A défaut de texte trouvé, c'est au responsable de traitements que cela revient. Pour déterminer cette durée, il faudra le faire en fonction de la finalité accomplie et pouvoir être en mesure de justifier ce choix auprès de la CNIL.

S'agissant du dossier du personnel, le droit du travail ne prévoit pas de durée d'archivage post départ du salarié en tant que tel.

La conservation du dossier du personnel après le départ du salarié est à déterminer en fonction de l'intérêt à les archiver.

Souvent, les employeurs ont intérêt à conserver ces données en cas de contrôle ou pour se ménager des preuves en cas de contentieux. En pratique, cette durée est souvent équivalente à 5 ans ; ce qui correspond à la durée de prescription civile de droit commun (article 2224 du code civil).

A l'inverse, le droit du travail encadre la conservation des bulletins de paie après le départ du salarié. En pratique, les durées post départ du salarié prévues par les textes correspondent à celles à retenir en archivage. **Ainsi, les bulletins de paie doivent être conservé 5 ans** après le départ du salarié s'agissant de ceux en format papier (article L. 3243-4 du code du travail).

Pour ceux en version dématérialisée, l'article D. 3243-8 du code du travail dit que l'employeur doit garantir de la mise à disposition au salarié de ses bulletins de paie durant 50 ans après son départ sauf si ce dernier s'y oppose. La méconnaissance de cette obligation par l'employeur est punie d'une contravention de 3ème classe (soit d'un montant de 450 euros) en vertu de l'article R.3246-2 du code du travail.

4. Les données personnelles pouvant être valablement collectées

Rappel sur les catégories de données spécifiques

Le RGPD consacre des catégories de données personnelles spécifiques et dont le traitement est interdit par principe :

- *Les données sensibles ;*
- *Les données de condamnations, d'infractions pénales et mesures de sûreté*

Pour les données sensibles, le RGPD prévoit des exceptions autorisant les responsables de traitements à en collecter dans certains cas (nécessité de la collecte pour exécuter les obligations en matière de droit du travail, pour plus d'infos, consulter le Référentiel RH de la CNIL).

Pour la seconde catégorie de données, l'article 46 de la loi Informatique et Libertés (le RGPD laissant aux Etats une marge de manœuvre sur ce sujet) prévoit qu'elles peuvent être collectées par :

- *les associations de défense de victimes agréée par le Ministère de la Justice*
- *les associations d'aide à la réinsertion des personnes placées sous-main de justice*
- *certains ESMS notamment ceux intervenant dans le domaine de la PJJ ou gérant des lieux d'accueil et de vie.*

- **Une association peut-elle demander un extrait de casier judiciaire à un administrateur bénévole ?**

En l'absence d'un texte spécifique, il n'est pas possible de conserver un extrait de casier judiciaire d'un candidat ou salarié. En revanche, il est possible de demander la présentation de l'extrait de casier judiciaire B3 à un administrateur bénévole sous réserve de procéder uniquement à sa vérification (et donc de ne pas le conserver). Si ce dernier ne veut pas le présenter alors que c'est une obligation légale ou règlementaire, l'association pourra légitimement interrompre la participation de l'administrateur bénévole.

5. La documentation de la mise en conformité

- **Les analyses d'impact sont-elles obligatoires seulement pour les entreprises de plus de 250 salariés et ce même en présence d'un traitement de données sensibles ?**

Rappel du cadre de la documentation de la mise en conformité

Le RGPD abolit les formalités administratives devant la CNIL pour les remplacer par un principe de protection des données dès la conception du traitement. Cela signifie que le responsable de traitements doit être en mesure de justifier la conformité du traitement tout au long de sa vie.

C'est pourquoi, un certain nombre de documents de conformité que le responsable de traitements doit tenir sont prévus par le RGPD.

Le premier document, le registre de traitements, recense tous les traitements de données mis en place par le responsable de traitements (dont ceux RH) et est obligatoire.

Le second, l'analyse d'impact sur la protection des données,n' est obligatoire que dans certains cas et pour les traitements les plus susceptibles de porter atteinte au droit à la vie privée des personnes concernées.

En matière de traitements de données personnelles RH, le référentiel de la CNIL dédié reprend la liste de traitements pour lesquels une analyse d'impact sur la protection des données (AIPD) n'est pas requises. C'est le cas des traitements RH mis en œuvre dans les conditions prévues par les textes applicables (principalement par le code du travail) et pour la seule gestion du personnel des organismes qui emploient moins de 250 personnes, à l'exception du recours au profilage. Lorsque l'employeur prévoit des traitements de données personnelles qui vont au-delà des conditions prévues par la loi, cela ne signifie pas automatiquement qu'une AIPD est obligatoire.

En effet, la méthode à suivre pour savoir si une AIPD est requise consiste à examiner si deux des 9 critères sont remplis :

- évaluation ou notation d'une personne ;
- prise de décision automatisée ;
- surveillance systématique ;
- traitement de données sensibles ou à caractère hautement personnel ;
- traitement à grande échelle ;
- croisement ou combinaison d'ensembles de données ;
- données concernant des personnes vulnérables ;
- utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles ;
- traitements qui empêchent les personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Au vu des règles applicables, un traitement de données sensibles en matière de ressources humaines en tant que tel n'implique pas la mise en place d'une AIPD. Cela pourra être le cas si un second critère est rempli.

Pour aller plus loin, **rendez-vous sur la page dédiée du site de la CNIL**.

Fédération
des acteurs de
la solidarité

https://www.federationsolidarite.org/

@FederationSolidarite

@FedeSolidarite

@federationsolidarite

Cette action est cofinancée par l'Union Européenne.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Direction générale de la cohésion sociale
Délégation générale à l'emploi
et à la formation professionnelle