

QUESTIONS/ REPONSES PROTECTION DES DONNEES PERSONNELLES

Ce FAQ contient les trois parties suivantes :

La première partie traite des notions générales en matière de protection des données personnelles, la deuxième partie décrit les droits des salariés en matière de protection des données personnelles et la dernière partie traite des obligations pesant sur les salariés en la matière.

1. Généralités

1.1 Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement par référence à un numéro d'identification (par exemple le numéro de sécurité sociale) ou par référence à un ou plusieurs éléments qui lui sont propres (par exemple les initiales du nom et du prénom) ou par recoupement d'informations du type : date de naissance, commune de résidence, éléments biométriques, etc.

1.2 Quel est le dispositif légal en matière de protection de données personnelles ?

La loi « Informatique et Libertés » du 6 janvier 1978 modifiée par la loi du 6 août 2004 est applicable dès lors qu'il existe un traitement automatisé ou un fichier manuel (c'est-à-dire un fichier informatique ou un fichier « papier ») contenant des données personnelle, c'est-à-dire des informations relatives à des personnes physiques et permettant directement ou indirectement leur identification.

Elle définit les principes à respecter lors de la collecte, du traitement et de la conservation de ces données et garantit un certain nombre de droits pour les personnes.

2. Les droits des salariés en matière de données personnelles

2.1 Quels sont les principes clés à respecter en matière de protection des données personnelles ?

- Le principe de finalité

Les données personnelles ne peuvent être recueillies et traitées que pour un usage déterminé et légitime. Tout détournement de finalité est passible de sanctions pénales.

Exemple : Les objectifs poursuivis par la mise en place d'une application informatique doivent donc être au préalable clairement définis (gestion des recrutements, sécurité du réseau informatique, contrôle du temps de travail, etc.).

- Le principe de proportionnalité et de pertinence des données

Seules doivent être traitées les informations pertinentes et nécessaires au regard des objectifs poursuivis.

Par exemple : le recueil d'informations sur l'entourage familial, l'état de santé ou encore le numéro de sécurité sociale d'un candidat à un recrutement n'est pas pertinent. L'enregistrement de la situation familiale précise d'un salarié ne peut se justifier que pour l'attribution d'avantages sociaux particuliers au salarié ou à sa famille.

En outre, comme le rappelle le Code du travail, la mise en place d'un dispositif de contrôle des salariés ne doit pas conduire à apporter de restrictions aux droits et libertés des personnes qui ne seraient pas proportionnées au but recherché et justifiées par l'intérêt légitime de l'entreprise.

Par exemple : la mise sous vidéosurveillance permanente d'un poste de travail ne pourrait intervenir qu'en cas de risque particulier et dûment avéré pour la sécurité du salarié concerné.

- Le principe d'une durée de conservation des données limitée

Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation précise doit être déterminée en fonction de la finalité de chaque fichier.

Par exemple : le temps de la présence du salarié s'agissant d'une application de gestion des carrières, cinq ans pour un fichier de paie, deux ans après le dernier contact avec le candidat à un emploi pour un fichier de recrutement, un mois pour les enregistrements de vidéosurveillance.

- Le principe de sécurité et de confidentialité des données

L'employeur, en tant que responsable du traitement, est astreint à une obligation de sécurité : il doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation à des tiers non autorisés.

Par exemple : chaque salarié doit disposer d'un mot de passe individuel régulièrement changé. Les droits d'accès aux données doivent être précisément définis en fonction des besoins réels de chaque personne (lecture, écriture, suppression). Il peut également être utile de prévoir un mécanisme de verrouillage systématique des postes informatiques au-delà d'une courte période de veille.

De plus, les données personnelles ne doivent être consultées que par les personnes habilitées à y accéder en raison de leurs fonctions.

Par exemple : les personnes habilitées du service des ressources humaines s'agissant de la gestion de la paie, les administrateurs réseaux s'agissant des données de connexion à internet.

Les données peuvent néanmoins être communiquées à des tiers autorisés à en connaître en application de dispositions législatives particulières (Inspections du travail, services fiscaux, services de police...).

- Le principe du respect des droits des personnes

-Information des personnes

Lors de l'informatisation de leurs données, les salariés concernés ou les candidats à un emploi doivent être clairement informés des objectifs poursuivis, du caractère obligatoire ou facultatif de leurs réponses, des destinataires des données et des modalités d'exercice de leurs droits au titre de la loi « Informatique et Libertés » (droit d'accès, de rectification et d'opposition).

-Droits d'accès et de rectification

Toute personne peut demander au détenteur d'un fichier de lui communiquer toutes les informations la concernant contenues dans ce fichier. Elle a également le droit de faire rectifier ou supprimer les informations erronées.

Par exemple : Sur simple demande et sans avoir à la motiver, un candidat ou un employé peut obtenir auprès de l'employeur une copie des données qui le concernent (recrutement, historique de carrière, rémunération, évaluation des compétences, dossier disciplinaire...) cf ci-dessous.

-Droit d'opposition

Toute personne a le droit de s'opposer, pour des motifs légitimes à ce que des données personnelles la concernant soient enregistrées dans un fichier informatique, sauf si celui-ci résulte d'une obligation légale ou réglementaire (ex. : déclarations sociales obligatoires, tenue du registre du personnel).

Par exemple : une personne peut dans certaines conditions s'opposer à la mise en ligne de ses coordonnées professionnelles ou de sa photographie.

2.2 Quelles données personnelles l'employeur peut-il collecter?

Dans le cadre d'un recrutement, les données collectées ne doivent servir qu'à évaluer la capacité du candidat à occuper l'emploi proposé (qualification, expérience, etc.).

À l'embauche du candidat, l'employeur pourra collecter des informations complémentaires. Outre celles nécessaires au respect d'une obligation légale (exemple : déclarations sociales obligatoires), l'employeur peut collecter des 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) ;
- à l'organisation du travail (par exemple, photographie facultative de l'employé pour les annuaires internes et organigrammes) ;
- à l'action sociale prise en charge par l'employeur (par exemple, les informations concernant les ayants-droit de l'employé)

2.3 Qui peut avoir accès aux données personnelles des salariés?

L'accès aux données personnelles des salariés doit être limité. Seules les personnes intervenant dans le processus de recrutement peuvent accéder aux informations d'un candidat.

Outre les administrations informées de l'embauche (exemple : assurance chômage, maladie, retraite, mutuelle...), seules les personnes chargées de la gestion du personnel peuvent consulter les informations des employés.

Les supérieurs hiérarchiques peuvent accéder aux informations nécessaires à l'exercice de leurs fonctions (exemple : données d'évaluations, rémunération...).

Les délégués du personnel ont accès aux données figurant dans le registre unique du personnel (nom, nationalité, fonction occupée, date d'entrée dans l'organisme, etc.).

Les autres instances (Comité d'entreprise, délégués syndicaux) peuvent obtenir certaines informations pour exercer leurs missions. Par exemple, l'employeur peut transmettre au Comité d'entreprise (CE), après information des employés, des données sur ceux qui ne s'y sont pas opposés. Ces informations permettront au CE de proposer des activités et des prestations adaptées.

Les organisations syndicales peuvent, après accord avec l'employeur, adresser aux employés des messages d'information syndicale par courrier électronique. Les employés peuvent s'y opposer à tout moment.

L'accès aux données personnelles doit être contrôlé.

L'employeur doit assurer la sécurité des informations et garantir que seules les personnes habilitées en prennent connaissance. Les actions sur les données effectuées par les personnes habilitées doivent être enregistrées (savoir qui se connecte à quoi, quand et pour faire quoi).

2.4 Comment exercer le droit d'accès au dossier professionnel ?

Tout salarié ou ancien salarié justifiant de son identité a le droit d'accéder à son dossier professionnel auprès du service du personnel.

Quelles données ?

L'intéressé peut obtenir communication de l'ensemble des données le concernant qu'elles soient conservées sur support informatique ou dans un dossier papier.

Par exemple il a droit d'accéder aux données relatives à :

- son recrutement
- son historique de carrière
- sa rémunération
- l'évaluation de ses compétences professionnelles
- son dossier disciplinaire

Limites au droit d'accès :

Le salarié ou ancien salarié n'a pas le droit d'accéder aux données concernant un autre salarié ou aux données prévisionnelles (potentiel de carrière, classement), sauf si ces données ont été prises en compte pour décider de son augmentation, de sa promotion etc.

L'employeur a le droit de s'opposer aux demandes manifestement abusives. En cas de contestation de la part du salarié, il doit démontrer que la demande du salarié est abusive.

Comment exercer le droit d'accès ?

Le droit d'accès peut s'exercer soit sur place soit par écrit. Lorsque la demande est effectuée par écrit, celle-ci doit être signée et accompagnée de la copie d'un justificatif d'identité.

L'employeur doit répondre dans un délai maximal de 2 mois. Son éventuel refus doit être écrit, motivé et doit mentionner les voies et délais de recours.

2.5 Mes données personnelles ont-elles été transférées dans une filiale située en dehors de l'UE ?

Les données personnelles des salariés de SOPRA HR SOFTWARE sont stockées dans la filiale tunisienne. On parle alors d'un « transfert de données vers un pays tiers ». Afin de garantir que les salariés qui bénéficient d'une protection de leurs données en UE continuent d'en bénéficier lorsque leurs données quittent l'UE, chaque filiale a conclu des clauses contractuelles types de l'UE. Depuis la mise en place des BCR au sein du groupe SOPRA HR SOFTWARE, il n'est plus nécessaire de conclure les clauses contractuelles types afin de garantir un niveau de protection suffisant aux salariés.

3. Mes devoirs quant aux données personnelles des clients du groupe SOPRA HR SOFTWARE

3.1 Règles à respecter par chaque salarié

- L'accès aux données personnelles ne doit se faire que conformément aux instructions de SOPRA HR SOFTWARE Solutions et de ses clients.
- Respect des mesures de sécurité et de confidentialité techniques et organisationnelles en place chez SOPRA HR SOFTWARE

Plus particulièrement :

- Ne pas utiliser les données personnelles auxquelles vous avez accès à d'autres fins que celles nécessaires à l'exercice de vos fonctions
- Ne pas vendre, céder, louer ou transférer les données personnelles auxquelles vous avez accès dans le cadre de vos fonctions sans obtenir l'accord exprès et préalable de SOPRA HR SOFTWARE
- Ne pas réaliser des copies des données personnelles sans l'accord exprès et préalable de SOPRA HR SOFTWARE (à moins que les copies soient nécessaires à l'exercice de vos fonctions)
- Informer immédiatement SOPRA HR SOFTWARE de tout accès accidentel ou non autorisé aux données personnelles ou plus généralement de tout manquement à la réglementation applicable en matière de données personnelles
 - Préserver la nature confidentielle des informations traitées

3.2 Quelles sont les sanctions en cas d'inobservation des règles énoncées sous le point 3.1 ?

- Sanctions disciplinaires
- Responsabilité civile (dommages-intérêts)
- Responsabilité pénale