IMPACTS DU RGPD* SUR LES SERVICES RESSOURCES HUMAINES (1/3)

*Règlement n°2016/679, dit règlement général sur la protection des données (GDPR : The EU General Data Protection Regulation).

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

Le RGPD est une règlementation européenne qui refond et renforce la protection des données à caractère personnel en conférant de nouveaux droits aux personnes physiques concernées.
Adopté le 27 avril 2016, entré en vigueur le 24 mai 2016 et applicable au 25 mai 2018, le RGPD s'applique à l'ensemble des traitements de données personnelles en concernant :

- toute organisation établie sur le territoire de l'Union (même si le traitement des données s'effectue depuis l'étranger),
- ainsi que toute organisation établie en dehors de l'Union Européenne traitant des données personnelles de personnes situées sur le territoire de l'Union.

L'adoption du RGPD a marqué un tournant majeur dans la régulation des traitements et flux de données personnelles en s'adaptant aux nouveaux enjeux technologiques et en renforçant le niveau de responsabilité de ceux qui ne respecteraient pas leurs obligations, notamment en matière de contrôle interne et d'analyse des risques.

Des données personnelles impliquées dans tous les Processus RH...

Recrutement
Onboarding
Formation
Carrières
Rémunération
Mobilité
Temps et activités
Congés
Notes de frais
Véhicules
Equipements
Litiges
Offboarding

1 Catégories de données

2 Services du responsable de traitement et destinataires

3 Finalités poursuivies

4 Fichiers

5 Durée de conservation

6 Fondement légal

7 Transferts

Carole Blancot (Désignation CNIL : N°DPO-37620 N°DPO-37624)
carole.blancot@spotpink.com - 06 50 86 29 33

IMPACTS DU RGPD SUR LES SERVICES RESSOURCES HUMAINES (2/3)

Information et consentement préalable des salariés

TRANSPARENCE ET LOYAUTÉ

L'employeur doit clairement informer les salariés du traitement de leurs données personnelles, et ce, à travers différents supports (règlement intérieur, contrat de travail, etc.).
La détention de certaines données requiert le consentement préalable de l'employé concerné. Celui-ci doit être obtenu de manière explicite et non équivoque pour les traitements concernés, notamment par un écrit ou une case à cocher (Art. 7 RGPD).

Principe de minimisation des données personnelles collectées

LIMITATION ET PROPORTIONNALITÉ

De manière générale, les données recueillies par l'employeur doivent être réduites au strict minimum et leur traitement proportionné à la finalité poursuivie (Art. 7 RGPD). Par exemple, les formulaires de candidature ne doivent imposer la divulgation de la situation matrimoniale d'un candidat ou de son numéro de sécurité sociale.
Des modalités particulières sont prévues pour les emplois où un extrait du casier judiciaire est nécessaire. Dans ce cas, l'employeur a l'interdiction de conserver ledit extrait ou des notes relatives à celui-ci.

Garantie de sécurité et de confidentialité des données

PROTECTION ET SÉCURITÉ DES DONNÉES

Le responsable du traitement doit déterminer et mettre en place les mesures techniques et organisationnelles nécessaires pour assurer la confidentialité des données personnelles des employés afin d'éviter toute divulgation (Art. 32 RGPD).
Toute faille de sécurité doit être signalée dans un délai de 72 heures à la CNIL ainsi qu'à l'employé concerné (Art. 33 et 34 RGPD).
Se pose également la question de savoir qui a accès aux données des employés au sein de l'entreprise. Il appartient à l'employeur de définir clairement les personnes destinataires et les données auxquelles les différents opérateurs des différents services de l'entreprise (et sous-traitants) ont légitimement accès, ainsi que de prendre des mesures organisationnelles et techniques pour cloisonner ces accès.

Application des droits des personnes

QUALITE ET EXACTITUDE

Le RGPD créé de nouveaux droits tels que le droit à la portabilité des données personnelles, le droit d'opposition ou le droit d'effacement (qui complètent les droits d'information, de limitation, d'accès et de rectification). Tout employé doit pouvoir saisir le service RH (ou le Délégué à la Protection des Données) pour faire l'exercice de ses droits détenus sur ses données personnelles.
Sa demande doit être suivie d'une réponse systématique rendue sous un mois (sauf pour une demande d'effacement dont l'effet doit être immédiat), ce qui implique la mise en place de mesures techniques adaptées pour respecter ce délai (Art. 3 RGPD), ainsi que la tenue d'un registre d'exercice des droits.

Carole Blancot (Désignation CNIL : N°DPO-37620 N°DPO-37624)
carole.blancot@spotpink.com - 06 50 86 29 33

IMPACTS DU RGPD SUR LES SERVICES RESSOURCES HUMAINES (3/3)

Principe de la conservation limitée des données

DURÉES MINIMALES ET MAXIMALES DE CONSERVATION ET D'ARCHIVAGE

Les données personnelles des salariés ne peuvent être conservées que pour la durée nécessaire (Art. 5 RGPD).
La politique de conservation des données est un projet stratégique et sensible car il porte sur le respect d'obligations légales et règlementaires (voire normatives), mais aussi car il peut affecter la capacité probatoire de l'entreprise.

Tenue de registres

(ENTREPRISES DE PLUS DE 250 SALARIÉS)

La CNIL n'a plus à être consultée en amont de tout traitement. L'employeur décide seul des traitements mis en place, mais il en est responsable et doit pouvoir les justifier en cas de contrôle de la CNIL. Les services RH doivent avoir recensé l'ensemble des données personnelles collectées et cartographier leurs traitements dans un registre. Celui-ci doit clairement répertorier les traitements relatifs aux ressources humaines, en déterminer la finalité, et préciser les mesures de sécurité et organisationnelles prises.
La CNIL peut prononcer diverses sanctions (susceptibles d'être rendues publiques) à l'égard des responsables de traitement qui ne respecteraient pas la Loi. **Le montant des sanctions pécuniaires peut s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial.**

Désignation d'un DPD (Délégué à la Protection des Données)

DPO-DPD : UN NOUVEL INTERLOCUTEUR

Le RGPD généralise la désignation d'un DPO (Data Protection Officer) pour toutes les entreprises de plus de 250 salariés, dès lors qu'elles effectuent des **traitements à grande échelle de suivi régulier et systématique des personnes ou de données sensibles** (Art. 37 RGPD).
Le DPO n'est pas obligatoire pour toutes les entreprises, toutefois, la complexité du traitement des données, rend la désignation du DPO plus que conseillée dans de nombreux contextes.
Le DPO peut être un salarié de l'entreprise ou un prestataire extérieur mais il convient d'éviter le conflit d'intérêt et de garantir l'indépendance de la personne désignée.

Profilage et prise de décisions automatisées

OBLIGATIONS SPÉCIFIQUES

Un traitement de profilage (Art. 4 RGPD) a pour objet d'évaluer une personne et de prédire ses réactions et ses préférences (comme par exemple déterminer ses performances au travail, sa situation financière, sa santé, ses préférences, ses habitudes de vie, etc.). Un traitement de profilage repose sur l'établissement d'un profil individualisé, concernant une personne en particulier. Il vise à évaluer certains de ses aspects personnels, en vue d'émettre un jugement ou de tirer des conclusions sur elle.
Il est en principe interdit de prendre une décision au sujet d'une personne si celle-ci est entièrement informatisée (sans intervention humaine) et si elle produit des effets juridiques à son égard ou si elle a un impact significatif sur elle (décision de recrutement ou non, décision d'augmentation ou non, etc.).

Carole Blancot (Désignation CNIL : N°DPO-37620 N°DPO-37624)
carole.blancot@spotpink.com - 06 50 86 29 33