

# Ressources Humaines : votre checklist pour protéger les données des employés

## Pourquoi sécuriser les données des employés ?

- Les RH traitent des données personnelles d'employés et de prestataires externes qui doivent être protégées, conformément au RGPD (Règlement Général sur la Protection des Données).
- Beaucoup de ces données sont partagées avec d'autres entités, elles aussi responsables de traitements : services généraux, finances, marketing et ventes, organismes publics...
- Certaines données sont particulièrement sensibles.
- Les RH jouent donc un rôle actif dans la mise en place du RGPD dans toute l'entreprise.



**95%** des services cloud utilisés par les RH sont inadaptés au RGPD<sup>1</sup>

**32%** des équipes RH sont impliquées dans le projet de mise en conformité<sup>2</sup>

**80%** des décideurs RH estiment que la confidentialité des données RH impacte fortement leurs missions<sup>3</sup>

1 : Netscope ; 2 : Proofpoint; 3 : Converteo

## Quels sont les usages des données RH ?

Les directions des Ressources Humaines créent et partagent de nombreuses données à caractère personnel.

- Annuaire d'entreprise, fonctions, photos
- Rémunérations, avantages, compétences
- Évaluations, formations, performances
- Santé, prévention des risques psychosociaux
- Gestion prédictive des compétences, tri de CV
- Gestion des droits et accès des employés, des externes, vidéosurveillance
- Transfert d'informations aux administrations, banques ou à d'autres services (marketing, finances, services généraux, opérations...)
- Formation des employés à la protection des données (article 39 du RGPD)

## Passer à l'action : la méthode de la CNIL en 6 étapes



Désigner un pilote



Cartographier vos traitements de données personnelles



Prioriser les actions à mener



Gérer les risques



Organiser les processus internes



Documenter la conformité



**Business  
Services**

## Checklist pour traiter les données des employés

- Participer activement au projet RGPD de l'entreprise
- Vérifier quelles règles nationales sont plus spécifiques que celles du RGPD
- Former les équipes RH et sensibiliser les autres entités également concernées : services généraux, finances...
- Faire l'inventaire des applications RH utilisées, répertoriées ou non par la DSI, mais aussi des documents Excel, Access...
- Mettre en place une authentification renforcée sur les traitements et systèmes critiques : double authentification, PKI...
- Déployer des requêtes directement intégrées aux SI pour éditer des rapports, et stocker ces derniers dans des espaces cloud sécurisés
- Limiter la transmission de données à caractère personnel entre entités (RH, services généraux, finances...), selon le principe de minimalisation du RGPD
- Rationaliser les listes de mailing utilisées en interne pour diffuser des informations relatives aux employés
- Informer les employés des droits sur les traitements de leur données : accès, rectification, oubli, délais de conservation
- Revoir les clauses sur la collecte des données à caractère personnel : règlement intérieur, contrat de travail, politique de sécurité...
- Rédiger un guide des bonnes pratiques RH en matière de données personnelles



### Orange Business Service, à vos côtés

- Accompagnement global de l'entreprise ou d'une direction à la mise en conformité au RGPD
- Conseil en transformation digitale des collaborateurs
- Sensibilisation, formation
- Gestion des habilitations
- Master Data Management
- Conseil en data intelligence



**Business  
Services**