

PROTECTION DES DONNÉES

DE QUOI S'AGIT-IL ?

Il s'agit de garantir la confidentialité, la sécurité et le stockage des données personnelles récupérées, analysées et conservées par l'entreprise. Cette thématique a pris beaucoup d'ampleur avec l'introduction des différentes lois régissant cette thématique, dont la nLPD à partir du 1^{er} septembre 2023.

PLUS-VALUE, ENJEUX

La plus-value s'inscrit notamment dans le respect de la loi, un renforcement de la confiance entre les employé-es et l'entreprise et une probabilité affaiblie de fuites de données sensibles.

4,62 millions USD	Coût total moyen d'une fuite de données liée à un ransomware	287 jours	Délai moyen pour récupérer une fuite de données	34 %	Pourcentage du nombre de fuites de données qui ont lieu avec l'aide d'une personne interne à l'entreprise
--------------------------	--	------------------	---	-------------	---

Source: Varonis 2022

LA DÉMARCHE ET LES OUTILS

La démarche consiste à :

- **Sensibiliser** les employé-es à ces thématiques principalement ceux et celles qui seraient amené-es à traiter ces données, mais cela peut s'étendre à un plus grand nombre.
- **Contrôler** de manière régulière le type de données récoltées, les processus mis en place et tenir à jour l'analyse des risques de ce mécanisme.
- **Gérer les accès** est primordial dans ce processus. En effet, il faut s'assurer que toutes les personnes qui peuvent atteindre ces éléments sont accréditées. C'est pourquoi un contrôle régulier est nécessaire, tant pour accorder de nouveaux accès que pour en retirer.
- **Sécuriser** comprend toutes les étapes. Il faut être certain que le niveau de sécurité corresponde à la confidentialité et la sensibilité des données stockées. En faisant des contrôles réguliers pour améliorer cela, le risque d'incidents est réduit.
- **Lorsque tout le processus est clair**, il est important de procéder à des tests afin de déceler les points à améliorer.



Toutes ces étapes peuvent être effectuées à des intervalles différents, mais ceux-ci doivent être réguliers. Il est recommandé de faire au minimum un contrôle annuel.

Pour s'assurer du suivi de ces contrôles, une check-list a été réalisée (ci-dessous). Celle-ci met en évidence les délais de conservations des données personnelles.

CHECK-LIST

10 ANS DE CONSERVATION

Pour les données suivantes:

- Données personnelles générales
- Contrat de travail
- Description des fonctions et du poste, cahier des charges
- Conventions de formation continue, plans de mesures
- Avertissements/réprimandes
- Résiliation
- Données salariales
- Correspondance importante et notes apportées par l'employeur
- Informations sur l'état de santé*

* dans certaines circonstances 20 ans après la fin des rapports de travail

5 ANS DE CONSERVATION

Pour les données suivantes:

- Décompte des vacances
- Contrôle du temps de travail/saisie des heures supplémentaires
- Données d'assurance

CAS PARTICULIERS

Pour les données suivantes:

- Évaluations de l'employé-e
Évaluations des trois à cinq dernières années: dix ans après la fin des rapports de travail
- Dossier de candidature
Aucun (restitution ou destruction à la fin des rapports de travail)

Source: [Insos](#)

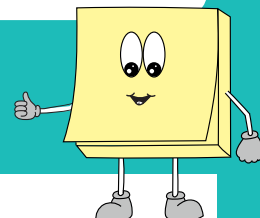
Des fiches complètes sont à disposition en annexe, il vous appartient de modifier et/ou d'ajouter les aspects que vous souhaitez contrôler.

CONSEILS

Primordial d'avoir des employé-es qui comprennent les enjeux et respectent les processus pour être en conformité avec les lois.

Contrôler que les documents et processus soient toujours en conformité afin de pouvoir réagir rapidement en cas de changement.

Procéder à des audits réguliers auprès des fournisseurs et partenaires s'avère être très important afin de s'assurer que tout le monde respecte les mêmes lignes directrices.



POUR ALLER PLUS LOIN

- Fiche annexe nLPD – un bref aperçu
- Fiche de contrôle/check-list pour la protection des données
- [Sécurité en ligne](#), guide de Swisscom
- [Check-list nouvelle loi sur la protection des données](#) – Kellerhals Carrard
- [Guide sur la conservation des données personnelles](#) – Insos