L’obligation de sécurité des données personnelles

—

NEO DPO

« La sécurité des données personnelles est un volet essentiel du RGPD : c'est une obligation qui pèse sur tout responsable de traitement et sous-traitant »

✓ **Art 32 du RGPD** :

1.Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre **les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
d)une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2.Lors de l'évaluation du niveau de sécurité approprié, **il est tenu compte en particulier des risques que présente le traitement**, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3.L'application d'un **code de conduite** approuvé comme le prévoit l'article 40 ou d'un **mécanisme de certification** approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

4.Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, **excepté sur instruction du responsable du traitement**, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

✓ Pour être pleinement pris en compte, l'obligation de sécurité doit être appréhendée de manière globale, sous l'angle des trois principes suivants :

- Le **principe de confidentialité** : les données ne doivent être accessibles qu'aux personnes autorisées
- Le **principe d'intégrité** : les données ne doivent pas être altérées ou modifiées
- Le **principe de disponibilité** : les données doivent être en permanence accessibles aux personnes autorisées

- ✓ On distingue les mesures de sécurité physique, logique et organisationnelle

- ✓ Les mesures doivent toujours être adaptées aux particularités du traitement et aux risques (par exemple, une base de données médicales ou un fichier de police nécessite davantage de mesures de sécurité qu'un fichier de membres d'un club de loisirs)

- ✓ Les mesures doivent être revues régulièrement pour être ajustées en fonction de l'évolution des risques

✓ Les mesures de sécurité physique :

- Sécuriser l'accès physique des locaux
- Sécuriser l'accès aux salles hébergeant les serveurs informatiques et les différents éléments du réseau

→Exemples de bonnes pratiques :

- Installer des alarmes anti-intrusion et les vérifier périodiquement
- Distinguer les zones des bâtiments selon les risques et tenir à jour une liste des personnes autorisées à entrer dans chaque zone
- Protéger physiquement les matériels informatiques par des moyens spécifiques : système anti-incendie dédié, surélévation en cas d'inondation, redondance d'alimentation électrique et/ou de climatisation
- Installer des serrures à chaque bureau et veiller à leur fermeture lors des absences

✓ Les mesures de sécurité logique :

- Adopter une politique rigoureuse de mot de passe pour l'accès aux postes de travail et à certains fichiers
- Sécuriser les postes de travail
- Tracer les accès à la base active et aux différentes archives
- Protéger le réseau informatique interne et les serveurs des attaques extérieures
- Anticiper le risque de perte ou de divulgation des données

→Exemples de bonnes pratiques :

- Définir un identifiant unique par utilisateur et interdire les comptes partagés
- Exiger des mots de passe robustes : la CNIL a publié une recommandation à ce sujet : https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires
- Bloquer temporairement l'accès au compte après plusieurs échecs
- Paramétrer les postes de travail pour qu'ils se verrouillent automatiquement à l'issue d'une courte période d'inactivité de l'utilisateur
- Prévoir un contrôle de l'usage des ports USB sur les postes sensibles
- Responsabiliser l'ensemble des acteurs en les informant de la mise en place d'une procédure de traçabilité des actions sur les fichiers, procéder au contrôle régulier des traces
- Mettre en place des dispositifs tels que les pare-feu et antivirus régulièrement mis à jour
- Pour les connexions à distance, utiliser des canaux sécurisés et des système d'authentification
- Limiter l'accès aux outils et interphases d'administration aux seules personnes habilitées
- Effectuer des sauvegardes régulières des données en prévoyant un stockage sur un site distinct
- Protéger les équipements de journalisation et les informations journalisées
- Chiffrer systématiquement les données stockés sur des supports nomades (smartphones, clé USB, portables)

✓ Les mesures de sécurité organisationnelle :

- Définir une politique de contrôle d'accès aux données
- Sensibiliser les utilisateurs sur les conditions d'utilisation des données
- Définir une politique de gestion des incidents touchant aux données personnelles
- Prévoir des audits réguliers des procédures et des traitements

→Exemples de bonnes pratiques :

- Définir les procédures à suivre à chaque mouvement de personnel (arrivée, départ ou changement d'affectation)
- Réaliser des revues régulières des droits accordés aux utilisateurs
- Prévoir des vérifications à effectuer en cas de demande d'un tiers de transmission des données (ex : police)
- Diffuser et faire signer à chaque utilisateur une charte informatique rappelant les conditions d'utilisation des équipements informatiques et des données personnelles
- Sensibiliser régulièrement les utilisateurs sur les règles (internes et pénales) et sur les menaces existantes
- Documenter les procédures d'exploitation des données, les mettre à jour et à disposition des utilisateurs
- Etablir une procédure en cas de vol, perte de support de données personnelles (personne à prévenir, dépôt de plainte etc.)
- Prévoir le ou les référents à saisir en cas d'atteinte à l'intégrité, la confidentialité et la disponibilité des données (Identification des mesures à prendre pour écarter ou limiter les risques d'impact sur les intéressés, question de la notification de la violation à la CNIL et aux personnes concernées)
- Identifier les traitements pertinents pour un audit interne ou externe régulier, établir un suivi de la mise en œuvre des mesures préconisées à la suite de ces audits
- Prévoir des critères de revue des analyses de risques (délai, avancée technologique, faille rendue publique etc.

- ✓ L'obligation de sécuriser les données doit conduire à mettre en place les mesures de sécurité physique, logiques et organisationnelles qui s'imposent

- ✓ Ces mesures devront être adaptées au contexte et, le cas échéant, réajustées en fonction de l'évolution du risque

- ✓ Pour aller plus loin :
  - Guide de la sécurité des données de la CNIL, contenant 17 fiches : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf
  - Guide d'hygiène informatique de l'ANSSI – renforcer la sécurité de son SI en 42 mesures : https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

Des questions ?

N’hésitez pas à me contacter

Rani ZAIDI – Consultant RGPD
DPO certifié Bureau Veritas

contact@neo-dpo.fr
06.63.61.38.68

www.neo-dpo.fr

NEO DPO