

Rapport de la Réglementation RGPD

Règlement Général sur la Protection des Données

Version 1 du 11 mars 2019

Ce règlement européen défini le 27 avril 2016; mis en vigueur en 2018 par cnil

Sommaire

I. Les enjeux	3
II. Le lien avec la cybersécurité	3
III. Les entreprises concernées	3
IV. La gestion des risques	3
V. Les missions	3
IV.1 Sensibiliser les utilisateurs	
IV.2 Authentifier les utilisateurs	
IV.3 Gérer les habilitations	
IV.4 Tracer les accès et gérer les incidents	
IV.5 Sécuriser les postes de travail	
IV.6 Sécuriser l'informatique mobile	
IV.7 Protéger le réseau informatique interne	
IV.8 Sécuriser les serveurs	
IV.9 Sécuriser les sites web	
IV.10 Sauvegarder et prévoir la continuité d'activité	
IV.11 Archiver de manière sécurisée	
IV.12 Encadrer la maintenance et la destruction des données	
IV.13 Gérer la sous-traitance	
IV.14 Sécuriser les échanges avec d'autres organismes	
IV.15 Protéger les locaux	
IV.16 Encadrer les développements informatiques	
IV.17 Chiffrer, garantir l'intégrité ou signer	
VI. Sanction en cas de transgression	
VII. Rôle de l'Entrepreneur	
VIII. Rôle du DPO	
X. Annexe	

I. Les enjeux

RGPD signifie Règlement Général sur la Protection des données. La protection des données personnelles nécessite de prendre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté à la cybermenace.

II. Le lien avec la cybersécurité

Chaque partie de la mise en conformité RGPD est liée avec la cybersécurité. Par exemple: comment protéger le réseau interne informatique, sécuriser les serveurs et chiffrer, garantir l'intégrité et signer, etc.

III. Les entreprises concernées

Toutes les entreprises stockent les données personnelles des citoyens européens. DPO vérifie la mise en conformité RGPD. Et après, il va contacter un cabinet tiers dans le domaine cybersécurité.

IV. La gestion des risques

Pour cela, de manière générale, il faut suivre des 4 étapes:

- Recenser les traitements des données sur les matériels, les logiciels, les canaux de commu et les supports papiers.
- Apprécier les risques engendrés par chaque traitement.
 - 1) Identifier les impacts potentiels
 - 2) Identifier les sources de risques
 - 3) Identifier les menaces réalisables
 - 4) Déterminer les mesures existantes ou prévues
 - 5) Estimer la gravité et la vraisemblance
- Mettre en oeuvre et vérifier les mesures prévues,
- Faire réaliser des audits de sécurité périodiques.

V. Les missions

IV.1 Sensibiliser les utilisateurs

IV.2 Authentifier les utilisateurs

IV.3 **Gérer les habilitations**

Les habilitations signifient les droits d'accès.

IV.4 Tracer les accès et gérer les incidents

IV.5 Sécuriser les postes de travail

IV.6 Sécuriser l'informatique mobile

IV.7 Protéger le réseau informatique interne

IV.8 Sécuriser les serveurs

IV.9 Sécuriser les sites web

- IV.10 Sauvegarder et prévoir la continuité d'activité
- IV.11 Archiver de manière sécurisée
- IV.12 Encadrer la maintenance et la destruction des données
- IV.13 **Gérer la sous-traitance**

Une entreprise distribue une tâche spécifique à l'autre entreprise; Dans le contrat, la cause de sécurité est bien définie.

- IV.14 Sécuriser les échanges avec d'autres organismes
- IV.15 Protéger les locaux
- IV.16 Encadrer les développements informatiques
- IV.17 Chiffrer, garantir l'intégrité ou signer

VI. Sanction en cas de transgression

Jusqu'à présent, une amende maximale de 50 000 euros est infligée par défaut intentionnel ou négligeant. À partir du 25 mai 2018, l'amende augmentait à 2% du chiffre d'affaires annuel global jusqu'à 10 millions euros. L'autorité de surveillance se réserve le droit d'imposer une amende plus élevée.

VII. Rôle de l'Entrepreneur

L'entrepreneur nomme le délégué à la protection des données conformément au règlement et s'engage à informer immédiatement l'autorité de contrôle.

VIII. Rôle du DPO

DPO, embauché par l'entrepreneur, possède toutes les qualifications appropriées pour garantir la conformité au règlement et s'engage à informer immédiatement à l'entrepreneur. Dès que les données sont échangées, un contrôle est nécessaire.

Au niveau européen, DPO est une personne chargée de garantir la conformité au règlement au sein d'une organisation.

X. Annexe

CNIL: Commission nationale informatique et libertés