DAMNET
EXPERTS .coop
INFORMATIQUES

MEMO GDPR-RGPD

Ce guide a pour vocation de sensibiliser et d'initier nos clients vers leur mise en conformité au Règlement européen relatif à la protection des données à caractère personnel. Ce règlement est appelé General Data Proctection Regulation (GDPR) ou Règlement Général sur la Protection des Données (RGPD).

Ce nouveau Règlement européen :

- Établit les règles relatives à la protection des données des personnes physiques à l'égard du stockage, des traitements, des archives et de la circulation de ces données (dans l'UE ou hors UE).
- Protège les libertés et droits fondamentaux des personnes physiques concernant la protection de leurs données à caractère personnel.
- Permet la libre circulation des données à caractère personnel au sein de l'UE pour des motifs liés à la protection des personnes physiques.

Dès lors, toute organisation est concernée par ce Règlement.

Pour vous aider à vous mettre en chemin vers cette conformité, voici un résumé des principales étapes.

1 – Choix d'un Coordinateur interne

Dans quelques cas, un « Délégué à la protection des données » sera obligatoire : si vous êtes un organisme public, si votre activité vous amène à manipuler des données personnelles à grandes échelles, ou à manipuler des données sensibles. Les données dites sensibles sont relatives aux enfants, à la santé, aux choix syndicaux, aux orientations religieuses ou sexuelles, au judiciaire.

Dans les autres cas, il est conseillé d'attribuer la charge de Coordination des actions liées à la protection des données à une personne qui connait bien votre organisation, qui a une bonne compréhension des enjeux informatiques et à la gestion des données en général, et qui sera formée au GDPR.

Ce Coordinateur aura notamment pour tâche :

- D'informer et de conseiller les personnes internes et les sous-traitants qui ont accès aux données concernées.
- De conseiller votre organisation préalablement à la conception d'un projet qui touche ces données.
- De coopérer avec l'autorité de contrôle le cas échéant.

2 – Registre des données détenues et leurs utilisations

Il s'agit de recenser précisément les données détenues ainsi que leurs traitements, dans des tableaux afin de légitimer, face aux parties prenantes, la détention des données ainsi que les types de traitements susceptibles d'être faits.

Ensuite, il s'agit de mener les actions nécessaires afin de limiter l'accès aux données et les traitements au strict nécessaire et le cas échéant, de veiller à pouvoir prouver le consentement des personnes concernées.

Damnet SCRL - R^te de Louvain-la-Neuve, 6/14 - 5001 Belgrade
Tel. : 081 21 51 50 - Fax : 081 21 50 78 – Belfius : BE81 0682 3303 2524
DAMNET.COOP

3 – Mesures de sécurité

Damnet peut vous aider à valider l'adéquation entre le risque encouru en cas de perte ou de vol de vos données et les techniques informatiques mises en œuvre dans votre entreprise. En cas de contrôle, de perte ou vol de vos données, vous serez amené à démontrer lors de la déclaration de la perte ou du vol que vos choix étaient proportionnés aux risques.

Cryptage des données
Le cryptage ou chiffrement (en français) des données est un procédé qui permet de rendre incompréhensible le contenu d'un document à toute personne ou système qui ne dispose pas de la clé de déchiffrement.
Dans le cadre du GDPR, le chiffrement des données est un moyen de répondre aux exigences légales en rendant inutilisables les données en cas de vol de ces dernières.

Gestion des utilisateurs et des accès
La confidentialité ne peut être garantie que si l'utilisateur est le seul à connaitre son mot de passe. Il ne faut en aucun cas tenir une liste de mots de passe. En cas de problème, l'administrateur du réseau peut toujours réinitialiser le mot de passe d'un utilisateur.
L'accès aux différents répertoires doit être sécurisé et accessible uniquement si la fonction du travailleur le demande. Une bonne gestion des accès permet de limiter les fuites de données confidentielles.

Protection des accès externes
Le Firewall ou pare-feu (en français) protège votre infrastructure informatique des attaques externes et protège donc vos données des accès non autorisés. Certains pare-feu permettent également une protection accrue en analysant le comportement des applications sur le réseau interne.
Des systèmes de monitoring permettent également d'analyser toutes les données brutes collectées sur une période définie afin d'identifier tout accès non autorisé.

Sauvegarde des données
Pour assurer la disponibilité et l'intégrité des données, il est important de mettre en place une politique de sauvegarde adaptée aux besoins de l'entreprise.
Il faut donc disposer d'un plan de sauvegarde précis et à jour et il est important de procéder à une revue régulière de l'activité de sauvegarde et de restauration.

4 – Implications internes

Pour garantir une bonne mise en œuvre au quotidien, une mise à jour régulière des mesures de protection des données, ainsi que l'accès à la documentation demandée en cas de contrôle, il serait judicieux de consigner des procédures internes impliquant notamment (liste non exhaustive) :

- ✓ Les méthodes de sensibilisation du personnel actuel et à venir à l'importance de prévenir le Coordinateur de toute anomalie observée et à l'organisation de la gestion de ces anomalies.
- ✓ Le processus de tenue à jour des Registres des données et des traitements.
- ✓ Le processus et le rythme des audits informatiques pour éprouver le niveau de sécurité de vos données
- ✓ L'analyse d'impacts potentiels en cas d'intrusion ou de perte de données et la marche à suivre en cas de perte ou vol de données.
- ✓ La consignation des consentements lorsque la raison d'être de la donnée n'est pas justifiée sur une base légale.
- ✓ D'intégrer les notions GDPR dans vos contrats avec vos clients et sous-traitants.
- ✓ De communiquer dans votre « Privacy Notice » les possibles utilisations des données détenues.
- ✓ La méthode claire et très accessible des demandes d'informations et des réclamations afin de permettre aux personnes d'exercer leurs droits.
- ✓ De veiller au respect du GDPR dès la conception de nouveaux projets impliquant des données personnelles.