RGPD : Concrètement, quelles mesures de sécurité prévoir ?

	RGPD : Concrètement, quelles mesures de sécurité prévoir ?

La Cnil rappelle les mesures à mettre en œuvre systématiquement sur la sécurité des données
La Commission nationale de l'informatique et des libertés (Cnil) publie un guide rappelant les précautions élémentaires à mettre en œuvre de manière systématique sur la sécurité des données personnelles.

Les 17 mesures de sécurité de base que l'on trouvera dans ce guide sont :
• Sensibiliser les utilisateurs ;
• Authentifier les utilisateurs ;
• Gérer les habilitations ;
• Tracer les accès et gérer les incidents ;
• Sécuriser les postes de travail ;
• Sécuriser l'informatique mobile ;
• Protéger le réseau informatique interne ;
• Sécuriser les serveurs ;
• Sécuriser les sites web ;
• Sauvegarder et prévoir la continuité d'activité ;
• Archiver de manière sécurisée ;
• Encadrer la maintenance et la destruction des données ;
• Gérer la sous-traitance ;
• Sécuriser les échanges avec d'autres organismes ;
• Protéger les locaux ;
• Encadrer les développements informatiques ;
• Chiffrer, garantir l'intégrité ou signer.

Pour information (et rappel pour ceux qui savent), l'article 32 du règlement européen sur la protection des données (RGPD), applicable au 25 mai 2018, prévoit :

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…

En résumé
Le responsable du traitement et le sous-traitant doivent prendre 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.

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Réagissez à cet article

Source : *La Cnil rappelle les mesures à mettre en œuvre systématiquement sur la sécurité des données • HOSPIMEDIA*