CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

ÊTES VOUS PRÊTS POUR LES NOUVELLES RÈGLES EN MATIÈRE DE PROTECTION DES DONNÉES?

10 questions pour aider votre institution à se préparer au Règlement Général sur la Protection des Données (RGPD)

POUR EN SAVOIR PLUS, VISITEZ WWW.CNPD.LU

Le Règlement Général sur la Protection des Données établira un régime unique de protection des données en Europe, remplaçant la directive de 1995 et la loi luxembourgeoise de 2002.

Êtes-vous au courant des nouveaux droits des individus et du renforcement de leurs droits existants?

Outre le renforcement des droits existants (p.ex. droit d'accès, droit de rectification), les responsables de traitements devront se préparer aux nouveaux droits des individus tels que l'élargissement du droit à l'effacement ("droit à l'oubli") et le droit à la portabilité des données. Avez-vous des procédures en place pour transférer les données à caractère personnel aux individus ou à d'autres organismes de manière électronique et dans un format "structuré et lisible par machine"?

Savez-vous que le RGPD sera applicable à partir du 25 mai 2018?

Bien que les lois existantes continueront de s'appliquer jusqu'à cette date, le moment est venu d'évaluer l'impact que le nouveau cadre juridique aura sur votre institution. Il est important d'allouer assez de temps et de ressources pour être en conformité avec le RGPD avant cette date.

Est-ce que votre institution est concernée?

Le RGPD ne sera pas seulement applicables aux institutions établies dans l'UE (responsables de traitements et sous-traitants), mais également aux entreprises hors de l'UE lorsqu'elles offrent des biens ou services sur le marché européen ou surveillent le comportement des résidents européens. Le RGPD sera donc applicable à des institutions qui n'étaient pas encore soumis au régime existant.

Êtes-vous au courant de vos activités de traitement des données à caractère personnel?

Un bon début pour développer une culture de la protection des données au sein de votre organisation est d'identifier et de documenter tous vos flux de données personnelles (p.ex. données des employés, des clients, etc.). Quelle est la base légale et la finalité des traitements existants? D'où proviennent ces données et qui en sont les destinataires? Où sont stockées les données et qui y a accès? Avec le RGPD, il sera nécessaire de tenir un registre détaillé des activités de traitement de données.

Est-ce que vous développez ou utilisez des produits ou services favorisant la protection des données?

Les institutions doivent adopter une approche de "protection des données dès la conception". Des garanties en matière de protection des données doivent être intégrées aux produits et services dès leur conception. Il sera nécessaire d'effectuer des analyses d'impact relatives à la protection des données pour les projets où les risques sont élevés. Dans certains cas, la CNPD devra être consultée avant de procéder au traitement. Il est également recommandé de se tenir informé des technologies renforçant la protection de la vie privée qui pourraient être pertinentes dans le cadre des activités de traitement de données de votre organisation.

Devrez-vous désigner un délégué à la protection des données?

Avec le RGPD, les entreprises qui effectuent certains traitements de données à grande échelle (p.ex. qui exigent un suivi régulier et systématique des individus) ainsi que les organismes et autorités publiques doivent obligatoirement désigner un délégué à la protection des données (DPD). Le DPD doit intervenir dans toutes les questions concernant la protection des données. Il serait opportun d'évaluer déjà maintenant si vous aurez besoin d'un DPD. Avez-vous des personnes au sein de votre organisation qui pourraient être en charge de la protection des données? Si non, avez-vous besoin d'embaucher quelqu'un?

Avez-vous mis en place des mesures de sécurité adaptées?

Avec le RGPD, vous devez documenter et revoir de manière regulière les mesures de sécurité en place. Pouvez-vous garantir un niveau de sécurité adapté aux risques liés aux traitements des données? Êtes-vous en mesure de restaurer les données à caractère personnel en cas d'incident? Comment garantissez-vous la confidentialité et l'intégrité des données sensibles?

Savez-vous que vous devez notifier les violations de sécurité à la CNPD endéans un délai de 72 heures?

Ce délai n'est obligatoire que si la violation en question est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées. Si ce risque est élevé, le responsable du traitement doit en plus communiquer la violation aux personnes affectées.

Si vous êtes un sous-traitant, vous devez avoir les bonnes procédures en place pour informer le responsable du traitement de la violation.

Savez-vous qu'il y aura des sanctions plus sévères pour les organisations en violation avec le règlement?

La CNPD, l'autorité de protection des données du Luxembourg, pourra infliger des amendes pouvant atteindre un montant maximal de 20 millions d'euros ou correspondant à 4% du chiffre d'affaire annuel mondial total du responsable du traitement en cas de traitement en violation avec les dispositions du règlement.

Devez-vous revoir et mettre à jour (si nécessaire) les contrats existants avec vos sous-traitants?

Les traitements de données effectués par un sous-traitant pour le compte du responsable du traitement doivent être régis par un contrat ou un autre acte juridique liant le sous-traitant au responsable du traitement. Le RGPD précise le contenu du contrat ou acte juridique.

Êtes vous un responsable du traitement ou un sous-traitant?

RESPONSABLE DU TRAITEMENT: détermine les finalités et les moyens du traitement de données à caractère personnel

SOUS-TRAITANT: traite des données à caractère personnel pour le compte du responsable du traitement

Commission nationale pour la protection des données
1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette
Tél.: (+352) 26 10 60-1
Fax: (+352) 26 10 60-29
E-mail: info@cnpd.lu