LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale,
de l'Enfance et de la Jeunesse

Centre de gestion informatique
de l'éducation

Luxembourg, le 9 janvier 2018

Référence: CGIE/DW/180109

NOTE IMPORTANTE

Mise en application du nouveau règlement européen GDPR

La mise en application du nouveau règlement européen GDPR (General Data Protection Regulation, règlement 2016/679) fixant les règles sur la protection des données à caractère personnel s'approche à grands pas.

Ce règlement européen est un texte à effet direct, c'est-à-dire qu'il n'y a pas besoin de loi nationale pour le transposer. Il sera directement applicable sur l'ensemble du territoire de l'Union européenne le 25 mai 2018. Le GDPR constitue l'une des plus vastes législations que l'UE ait adoptées ces dernières années, et un certain nombre de concepts à mettre en œuvre, tels que le terme registre des traitements, analyse de risque, droit à l'oubli numérique, la portabilité des données, la notification des violations de données, et la responsabilité dite "accountability" (pour n'en citer que quelques-uns) nécessiteront un certain temps d'adaptation.

Les règles et obligations du GDPR s'appliquent au traitement – automatisé ou non – des données à caractère personnel. L'objectif du GDPR est de renforcer l'encadrement des pratiques en matière de collecte et d'utilisation des données à caractère personnel.

La logique du nouveau règlement est la suppression des formalités préalables auprès des autorités nationales de contrôle (CNPD). Il n'y a donc plus de déclaration ou de demandes d'autorisation préalable à la mise en place de traitements de données à caractère personnel.

Cependant, à partir du 25 mai 2018, le responsable du traitement (celui qui prend l'initiative de (faire) collecter et tenir des données à caractère personnel) a l'obligation de mettre en œuvre des mécanismes et des procédures permettant de démontrer le respect des règles relatives à la protection des données.

Concrètement, les spécifications mêmes des applications qui traitent les données et leurs procédures d'exploitation devront prendre en compte les règles de protection des données personnelles édictées par le règlement. Cette documentation devra exister et être mise à disposition de la CNPD en cas de contrôle.

De plus, chaque responsable de traitements doit mettre en place un « registre des traitements de données » contenant un certain nombre d'informations au sujet des traitements de données d'une entité. Dans ce contexte, l'État luxembourgeois met à disposition l'application « **DataREG** » qui sert à enregistrer tous traitements de données à caractère personnels grâce à des fiches d'inventaires.

Lorsqu'un traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer une analyse d'impact de ce dernier sur la protection des données à caractère personnel. L'application DataREG permet d'identifier automatiquement les traitements de données pouvant engendrer un risque de perte de données personnelles et nécessitant une analyse d'impact.

Dans le contexte du GDPR, entre autres, les mesures suivantes sont à prendre par le responsable du traitement :

- La mise en place de procédures internes permettant de garantir le respect des principes de protection des données (notamment lors de la création de la modification, ou de la suppression d'un traitement) ;
- L'inventaire des traitements de données personnelles ;
- La répartition des rôles et responsabilités ;
- La sensibilisation et la formation du personnel ;
- La vérification de l'efficacité des mesures (indicateurs de performances, audits) ;
- La transparence sur la gestion des plaintes ;
- La mise en place d'un code de conduite ;

Il convient enfin de noter que le seul fait de ne pas fournir les éléments attestant de la conformité du/des traitements(s) concerné(s) est susceptible d'entrainer une sanction, indépendamment de l'existence ou non d'une violation des données.

Concernant les sanctions, deux seuils sont fixés en cas de non-conformité au règlement européen suivant la nature de l'infraction (l'article 79 du règlement détaille la liste des infractions pour chacun des seuils :

- Un premier seuil à 2% du chiffre d'affaire mondial ou 10 millions d'euros (maximum des 2 valeurs) pour les infractions mineures : absence de registre des traitements, non nomination d'un DPO si elle est obligatoire ou encore non réalisation des analyses d'impact

- Un deuxième seuil à 4% du chiffre d'affaire mondial ou 20 millions d'euros (maximum des 2 valeurs) pour les infractions les plus graves : non recueil du

consentement, non-respect des droits des personnes, transfert international illégal ou encore non-respect d'une interdiction de mise en œuvre d'un traitement.

Le montant des amendes dépendra de la nature de l'infraction ainsi que de l'éventuelle récidive du responsable de traitement.

Afin de se rendre conforme au nouveau règlement, le CGIE conseille aux différentes entités d'implémenter la Politique de Sécurité de l'information de l'État luxembourgeois (PSI-LU) élaborée par l'ANSSI (Agence Nationale pour la Sécurité d'Information) et qui a été approuvée par le Conseil de gouvernement en date du 16 mars 2016.

Cette politique permet de mettre en application la stratégie de cyber sécurité approuvée et rendue exécutoire par le conseil du gouvernement et de répondre aux exigences de la norme ISO/IEC 27001. En plus de la Politique de Sécurité de l'Information de l'État luxembourgeois (PSI-LU), cette mise en application repose également sur l'implémentation d'un **Système de Management de la Sécurité de l'Information (SMSI)** selon la norme ISO/IEC 27002). Cette implémentation offre une démarche pertinente pour améliorer la sécurité de l'information d'une entité et de réduire les risques associés.

Le CGIE travaille depuis un an sur le processus d'implémentation du SMSI qui nous amène à revoir nos mesures de sécurité organisationnelles et techniques et des mettre en place des optimisations conséquentes afin de répondre aux exigences et aux recommandations de la PSI-LU et du SMSI.

En restant à votre disposition pour tout renseignement complémentaire, je vous prie d'agréer, Madame, Monsieur, l'expression de ma parfaite considération.

Daniel Weiler
Directeur