AVIS
D'EXPERT

Sécurité des données :
Quels impacts du Règlement Général sur la Protection des Données Personnelles adopté par l'Union Européenne?

Le Parlement européen a adopté en avril 2016 le Règlement Général sur la Protection des Données Personnelles (ou General Data Protection Regulation ou GDPR), la plus importante réforme de la législation européenne en matière de protection des données personnelles de ces vingt dernières années. **Directement applicable dans tous les états membres de l'Union Européenne, il impose les mêmes règles pour tous, à compter du 25 mai 2018.** Les entreprises et les organisations concernées sont européennes et non européennes, du moment qu'elles collectent, traitent ou stockent des données personnelles de citoyens européens.

Sous l'effet de la transformation digitale, les fuites de données personnelles explosent. D'après les résultats du « 2016 Data Breach Investigations Report », plus de 90% des « vols » de données contiennent des données personnelles. Les scandales sur des fuites de données compromettant la sécurité et la vie privée des clients ou utilisateurs des organisations ciblées font la une des médias ces derniers mois. En septembre 2016, Yahoo a révélé le vol record des données personnelles de 500 millions de comptes.

Face à ces enjeux, les organisations concernées ont désormais moins d'un an pour se conformer aux exigences du GDPR. Au-delà des importantes sanctions encourues, cette nouvelle législation introduit de **nombreuses obligations dans le domaine de la sécurité des systèmes d'information (SI) traitant de données à caractère personnel**.

Une amende jusqu'à 20 millions d'euros ou 4% du CA mondial en cas de non-respect du GDPR.

La sensibilisation ainsi qu'une étude des impacts spécifiques du GDPR sur la sécurisation du SI est donc nécessaire. Le présent avis d'expert en expose néanmoins les principales règles.

Assurer la sécurité du traitement des données personnelles

Une obligation globale de sécurité

En tant que responsables de traitement de données à caractère personnel, les organisations devront mettre en œuvre « **les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté** » aux données, en considération des risques pour les individus concernés « résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données ».

À titre d'orientations pratiques, le texte met l'accent sur la pseudonymisation, le chiffrement des données tout au long de leur cycle de vie et l'évaluation régulière des mesures de sécurité, par exemple par des audits.

La notification des incidents de sécurité

Les organisations devront signaler toute violation de la sécurité de données à caractère personnel à l'autorité de contrôle (en France, la CNIL) sous **72 heures**. Elle sera également tenue d'informer les individus dont les données personnelles ont été compromises si la violation porte atteinte à leurs droits et libertés. Les impacts peuvent être considérables en termes d'image et les conséquences parfois durables sur la réputation de l'organisation.

Une coresponsabilité des prestataires

Face au développement de l'externalisation complète de certains services et l'émergence du mode SaaS, le texte introduit la notion de responsabilité conjointe du responsable de traitement et du sous-traitant. Ce dernier est tenu d'apporter les garanties suffisantes en termes de sécurité des données qui lui sont confiées et de notifier à son client toute violation des données à caractère personnel.

Assurer la sécurité en amont du traitement

L'analyse des risques liés au traitement

L'analyse d'impact des traitements (**Privacy Impact Assessment ou PIA**) sur la protection des données personnelles prévoit l'analyse des risques sécurité affectant le système d'information et des conséquences des violations de sécurité pour les individus concernés.

La protection des données intégrées aux projets

Reposant sur une logique de responsabilité (« accountability »), le texte prévoit deux notions primordiales :

• « **Privacy by design** » signifie que la protection des données personnelles, par des mesures techniques et organisationnelles, devra être prévue dès la conception d'un produit ou d'un service. Le déploiement rapide des PIA permettra de minimiser les risques de faille de sécurité au démarrage des projets.

• Le **« Privacy by default** » implique que le responsable du traitement mette en œuvre, par défaut, toutes les mesures nécessaires pour protéger les données au regard de la finalité du traitement.

Quelles étapes pour se mettre en conformité ?

Afin d'accompagner les organisations dans leur mise en conformité et leur permettre d'en apporter la preuve, la CNIL a publié en mars dernier une méthodologie en 6 étapes en matière de sécurisation du SI et de protection des données :

• **Adapter la gouvernance** interne au GDPR en nommant un Data Protection Officer, en s'assurant de la collaboration efficace avec le RSSI et en intégrant la protection des données à caractère personnel dans la politique de sécurité et dans la classification des données de l'entreprise,

• **Cartographier les traitements** des données personnelles et identifier les transferts hors UE,

•Adopter une **approche par le risque** en intégrant la protection des données, et en particulier le PIA, le Privacy by Design et le Privacy by Default, dans le cycle et la méthodologie des projets informatiques,

• Contrôler les **opérations de sous-traitance informatique et d'externalisation du SI** pour s'assurer de la bonne prise en compte des obligations de sécurité des prestataires,

• Mettre en place les procédures internes adaptées pour la gestion et la **notification des incidents de sécurité** impliquant la compromission de données personnelles,

• Maintenir la documentation assurant la **traçabilité des données et des mesures de sécurisation** mises en œuvre (ex : registre de traitements, PIA, etc).

Le nouveau règlement montre bien l'intention du législateur européen d'harmoniser (voire élever) le niveau de sécurité des données au sein de l'Union Européenne et de l'adapter aux avancements des nouvelles technologies et à la transformation digitale.

La mise en conformité au GPDR peut contribuer à la réalisation de la stratégie de l'organisation par l'amélioration continue du niveau de sécurité, mais aussi en étant un investissement dans la confiance -élément essentiel de la réussite de sa transformation digitale-, voire un avantage compétitif, en optimisant les outils de conformité.

Auteur

Jean-Philippe CASSARD

Docteur en droit

Responsable conformité règlementaire

Expertises :

- *Droit du numérique / cybersécurité*
- *Règlementations françaises et européennes (NIS / LPM, GDPR / CNIL, eIDAS, export control, …)*
- *Conseil en cybersécurité*