Anticiper la conformité au nouveau Règlement Général sur la Protection des Données

Un élément incontournable de la gestion des risques de votre organisation !

Patrick Soenen, Associé audit informatique, Crowe Horwath | Callens, Pirenne, Theunissen & C°

Un défi majeur auquel la gestion des risques des entreprises doit faire face, aujourd'hui est celui qui consiste à protéger les données à caractère personnel (par exemple fichiers de clients ou du personnel). Son importance croît proportionnellement aux exigences du nouveau Règlement Européen sur la Protection des Données.

Le Règlement Général sur la Protection des Données

Le RGPD (2016/679) a été adopté par le Parlement Européen et le Conseil de l'Europe le 27 avril 2016 et a été publié au Journal Officiel le 4 mai 2016. Il sera applicable le 25 mai 2018 dans tous les pays de l'Union Européenne. Le règlement remplace la directive européenne de 1995 sur la protection des données à caractère personnel (95/46/CE). Cette législation unique met fin à la fragmentation juridique actuelle entre les états membres et permettra à l'Europe de s'adapter aux nouvelles réalités du numérique.

La notion de « donnée à caractère personnel » couvre toute information se rapportant à une personne physique identifiée ou identifiable, dénommée « personne concernée ». Une personne concernée est une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Est interdit le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Les changements majeurs

Les principaux changements par rapport à la directive européenne 95/46 peuvent se synthétiser en 9 points d'attention incontournables, repris dans le schéma 1.

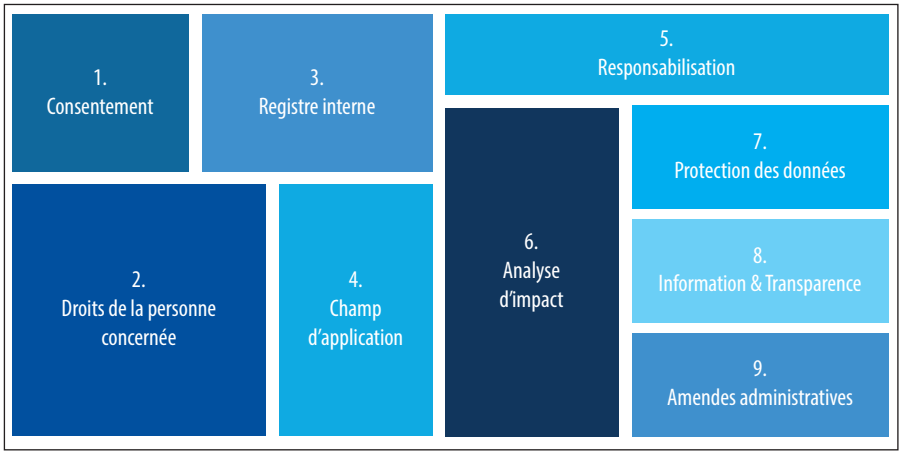

Schéma 1 : Les changements majeurs.

1. Le « **consentement** » de la personne concernée est toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle celle-ci accepte par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles.

2. La personne concernée a **le droit** d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées, la rectification des données à caractère personnel qui sont inexactes, la limitation du traitement, et l'effacement (droit à l'oubli). La personne concernée a également le droit de s'opposer à tout moment à un traitement des données à caractère personnel la concernant (droit d'opposition), et de recevoir les données à caractère personnel la concernant dans un format structuré, couramment utilisé et lisible (droit à la portabilité).

3. Le responsable du traitement tient un **registre interne** des activités de traitement effectuées sous sa responsabilité, et chaque sous-traitant tient également un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement.

4. Le règlement **s'applique** au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.

5. Le règlement s'applique aux responsables du traitement et aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel. La **responsabilisation** *(accountability)* implique que le responsable du traitement met en œuvre des mesures efficaces et appropriées afin de se conformer au règlement européen et d'apporter la preuve, sur demande de l'autorité de contrôle, que les mesures appropriées ont été prises. Les éventuels sous-traitants doivent présenter des garanties suffisantes quant à la mise en œuvre de mesures appropriées équivalentes.

6. Lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une **analyse de l'impact** des opérations de traitement envisagées sur la protection des données à caractère personnel. Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsque l'analyse d'impact indique que le traitement présenterait un risque élevé.

7. En matière de **protection des données,** le responsable du traitement adopte des mesures techniques et organisationnelles appropriées qui sont destinées à mettre en œuvre les principes relatifs à la protection

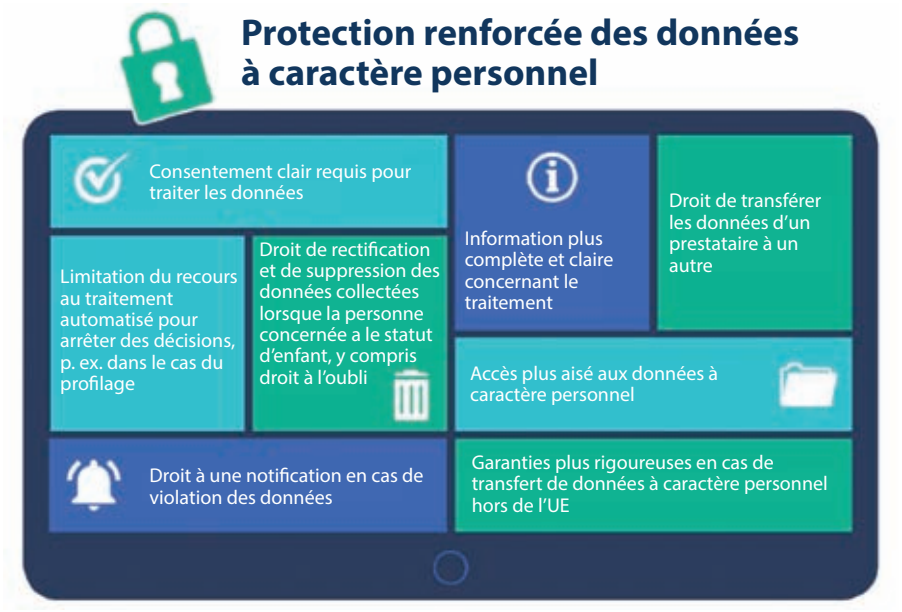

Schéma 2 : Protection renforcée des données à caractère personnel..

Schéma 3 : Perspectives pour les entreprises..

des données (protection dès la conception), ainsi que les mesures pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées (protection par défaut). Le responsable du traitement et le sous-traitant mettent également en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Le responsable du traitement et le sous-traitant désignent un **Délégué à la Protection des Données** notamment lorsque le traitement est effectué par une autorité publique ou un organisme public, ou lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées.

8. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées, le responsable du traitement lui fournit lors de la collecte des **informations** détaillées concernant notamment l'identité et les coordonnées du responsable du traitement ; le cas échéant, les coordonnées du Délégué à la Protection des Données ; les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement.

Dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite, il la notifie à l'autorité de contrôle compétente si possible, 72 heures au plus tard après en avoir pris connaissance. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement devra communiquer la fuite à la personne concernée dans les meilleurs délais.

9. La responsabilisation passe par un renforcement des pouvoirs de sanction de l'autorité de contrôle. Les violations font l'objet d'**amendes administratives** pouvant s'élever jusqu'à 10 millions € ou jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent pour les infractions de non-conformité et jusqu'à 20 millions € ou jusqu'à 4 % de ce chiffre d'affaires pour les infractions liées aux violations de données. Mais l'interdiction de traitement des données personnelles pourrait constituer une sanction bien plus handicapante.

> ***« Le Délégué à la Protection des Données - un acteur clé de la deuxième ligne de maîtrise »***

Les principales responsabilités

Transformer le risque de non-conformité au nouveau Règlement Général sur la Protection des Données en opportunité est pour le conseil d'administration et le comité exécutif un axe de gestion clé s'ils peuvent démontrer aux parties prenantes leur engagement vis-à-vis des exigences. Pour ce faire, désigner dès à présent les rôles et responsabilités est une des premières étapes de l'implémentation.

Le Délégué à la Protection des Données : un acteur clé de la deuxième ligne de maîtrise

Le Délégué se substitue au Correspondant Informatique et Libertés (CIL) et se voit doté de compétences élargies. Le Délégué à la Protection des Données devra agir dans le respect des principes d'absence de conflit d'intérêts, de confidentialité, d'indépendance et de secret professionnel, pour assister les organismes et faire appliquer le traitement des données conformément au règlement européen. Il sera chargé de :

- Informer et conseiller le responsable de traitement ou le sous-traitant sur les obligations qui lui incombent en matière de protection des données ;
- Contrôler le respect de la législation applicable en matière de protection des données et des règles internes du responsable de traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;
- Dispenser des conseils sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci ;
- Coopérer avec l'autorité de contrôle ;
- Faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement et mener des consultations, le cas échéant.

La Direction des Systèmes d'Information : un rouage de la mise en œuvre

La mise en œuvre de la réglementation implique une révision complète des processus des traitement de données à caractère personnel. Tout développement de logiciel devra prévoir la protection des données dès la conception et la protection par défaut. Ces obligations entraînent pour la DSI la nécessaire conformité « du la conception du logiciel jusqu'à sa mise en œuvre opérationnelle ».

Le Responsable de la Sécurité des Systèmes d'Information : un incontournable du principe de sécurisation

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 :

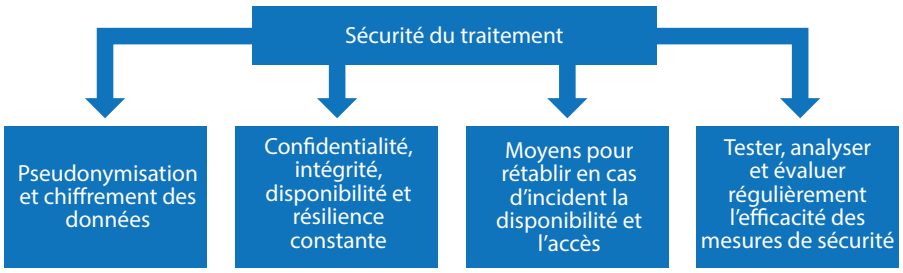

Schéma 4 : Mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Le Service Juridique : essentiel dans le conseil et l'accompagnement

Le service juridique joue un rôle essentiel dans la gestion des données à caractère personnel. Il conseille, accompagne et met en garde les opérationnels : rédaction des mentions légales, négociation de contrat, guide des bonnes pratiques en matière de protection des données, sensibilisation à la protection des données...

La mise à conformité à anticiper !

Les organisations doivent déployer **dès maintenant** les bases d'une stratégie efficace de protection des données pour être en conformité lorsque le règlement entrera définitivement en vigueur le 25 mai 2018.

En effet, le règlement prévoit l'exercice du principe de protection des données personnelles au travers de la protection renforcée (droits des personnes), la protection analysée (analyse d'impact), la protection en amont (avec les principes de protection par conception et par défaut), la protection en chaîne (responsabilité du sous-traitant et possibilité de coresponsabilité) et la protection documentée (documentation obligatoire en tant que preuve de la conformité légale). La mise en conformité peut donc représenter une charge de travail importante très dépendante du secteur d'activité.

Pourquoi démarrer dès aujourd'hui ? Pour avoir le temps de cartographier vos données à caractère personnel, de mettre en place des processus et des plateformes informatiques « sécurisés », de désigner un délégué à la protection des données, d'analyser les risques d'impact, de former vos collaborateurs à la collecte des données, d'obtenir le consentement des personnes concernées, de mettre à niveau les contrats avec vos sous-traitants, de réaliser des audits pour vérifier votre conformité au regard des nouvelles directives, … Tout un programme ! ■

Retrouvez le texte intégral du Règlement Européen sur la Protection des Données sur le site de la CNIL : https://www.cnil.fr/reglement-europeen-protection-donnees