RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Applications du RGPD en SSTI

Le RGPD (Règlement Général sur la Protection des Données) sera applicable à compter du 25 mai prochain et concernera directement les SSTI.

Responsable de la sécurité des données chez AXESS Solutions Santé, Madame Aurélie Tracol est venue exposer à la Commission Système d'Information de Présanse les grands principes du RGPD et sa mise en application dans les Services.

Rédigé en anglais et constituant le texte européen de référence en matière de protection des données à caractère personnel au sein de l'Union Européenne, le RGPD comprend 99 articles et sera applicable à compter du 25 mai 2018, remplaçant la directive CE 95-46 du 24 octobre 1995.

Auparavant, la directive de 1995 était transposée dans 28 lois différentes, une par État membre (par exemple transposée dans la loi Informatique et Liberté), et s'avérait peu efficiente auprès des grandes entreprises.

Le RGPD concerne aussi bien les données informatiques que le format papier, renforce le droit des personnes, ainsi que la responsabilisation des entités (responsabilité dans le traitement des données et responsabilité des sous-traitants). Il augmente en outre les possibles sanctions financières pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires d'une entreprise. Le montant de la sanction étant le plus élevé des deux.

Quelques définitions pour rappel :

Données à caractère personnel : il s'agit de l'ensemble des informations qui permettent d'identifier directement ou indirectement une personne.

A titre d'exemple, depuis un arrêt de la Cour de cassation de novembre 2016, les adresses IP sont considérées comme des données à caractère personnel.

Les moyens mis en œuvre par le responsable du traitement peuvent être l'anonymisation ou la pseudonymisation. Dans ce dernier cas, il est possible, par l'utilisation d'un algorithme, de retrouver les données d'origine.

Données sensibles : le RGPD parle de données personnelles particulières. Il s'agit de données personnelles, en particulier celles relatives à la santé, y compris les prestations de soin. Le traitement des données sensibles est en général interdit par le RGPD sauf cas particuliers. Parmi ceux-ci figurent les traitements aux fins de la médecine du travail.

Traitement : on entend par traitement tout processus mis en œuvre sur des données, y compris leur conservation.

Responsable du traitement : il s'agit de la personne qui détermine les finalités et les modalités du traitement.

Les grands principes du RGPD

Les grands principes du RGPD sont au nombre de 7 :

- **Responsabilisation**

Le RGPD invite les entreprises à prendre les mesures nécessaires pour la conformité des traitements et à être en mesure de le démontrer.

Pour cela, un registre de traitements doit être tenu à jour. La mise en œuvre du RGPD remplace le dépôt de dossier auprès de la CNIL.

- **Coresponsabilité des sous-traitants**

Les sous-traitants doivent s'engager contractuellement et sont solidairement responsables.

- **Protection de la vie privée dès la conception (privacy by design)**

Cette protection doit être effective tout au long de la durée de vie des données.

- **Protection de la vie privée par défaut (privacy by default)**

Cette protection est appelée à être mise en œuvre au plus haut niveau. La collecte des données doit faire l'objet d'un consentement éclairé et explicite, la conservation des données ne peut se faire que pour une durée limitée. Enfin, l'accès à celles-ci doit faire l'objet d'habilitations.

- **Analyse d'impact sur la vie privée (privacy impact assessment)**

Il convient de procéder à une analyse des risques vis-à-vis des droits et des libertés dans le cadre d'une collecte massive de données.

- **Désignation d'un délégué à la protection des données (DPO)**

Ce DPO peut être interne à l'entreprise ou externalisé, mutualisé. Lorsque le DPO est un personnel de l'entreprise, il bénéficie du statut de salarié protégé.

Signalement des violations de données personnelles

En cas d'intrusion dans la base de données, de pertes/vols d'ordinateurs, de supports de stockage ou encore de téléphones portables, un signalement doit être fait auprès de la CNIL dans les 72 heures, puis auprès de la/des personne(s) concernée(s).

Nouveaux droits des personnes

Dans le cadre du RGPD s'ajoutent aux droits déjà existants, le renforcement de l'information des personnes (consentement), un droit à l'oubli, un droit à la limitation de traitements, un droit à la portabilité des données (structurées et lisibles – formats).

Les applications du RGDP en SSTI

La CNIL reste l'autorité de contrôle pour le RGPD et l'ensemble des personnels des SSTI est potentiellement concerné par le RGPD (personnels RH, personnels en charge de la gestion des adhérents et des convocations, personnels juridiques, personnels techniques, ...).

La mise en conformité peut être effectuée en six étapes :

Désigner un pilote (DPO)

Il est conseillé de privilégier un profil mi-technique, mi-juridique et de travailler en coopération avec la CNIL. Le DPO constitue un nouveau métier. A ce titre, quelques 80 000 recrutements sont prévus.

Cartographie des traitements

Un registre doit être tenu, qui doit comporter les personnes qui ont accès aux données, en précisant les données concernées et la raison du/des traitement(s), ainsi que la description de ceux-ci, de même que la durée du/des traitement(s).

En outre, il convient de prendre en compte la durée de conservation, le lieu de stockage ou encore de lister les mesures de sécurité pour minimiser les risques.

Prioriser les actions

Il convient de s'interroger sur les données réellement utiles, d'identifier la base juridique, ...
Dès lors, il apparaît nécessaire de réaliser un audit pour vérifier et prioriser les actions.

Gérer les risques

Il convient d'analyser les impacts possibles sur la vie privée. Pour ce faire, un outil (PIA) est accessible en ligne sur le site Internet de la CNIL.

Organiser les processus

Tous les personnels du Service doivent être sensibilisés à l'utilité du RGPD. Cette information doit également être dispensée aux sous-traitants. Pour ce faire, une charte peut être établie.

Documenter la conformité

Il est nécessaire d'être en mesure de prouver à tout moment des actions mises en œuvre dans le cadre du RGPD (documents sur le traitement, informations dispensées aux personnes, contrôles et responsabilités des acteurs, ...).

En conclusion, la mise en application du RGPD constitue une opportunité vers plus de protection des données personnelles, inscrivant ainsi le droit à la vie privée comme un droit fondamental.

De plus, le RGDP permettra de renforcer la position des SSTI comme tiers de confiance et son usage devrait améliorer l'efficacité des SSTI dans leur offre aux entreprises et aux salariés.

La mise en conformité des SSTI au RGPD sera réussie si :

- l'ensemble des personnels des SSTI sont convaincus qu'il permettra de renforcer les SSTI et de pérenniser leur indépendance et leur rôle,
- la transition est organisée, notamment en faisant appel, si besoin, à la CNIL,
- une communication efficace est mise en place afin de sensibiliser l'ensemble des collaborateurs,
- une démarche de suivi dans le temps avec une volonté d'amélioration continue est mise en œuvre. A ce titre, le RGPD pourra s'articuler avec les certifications (ISO, AMEXIST, ...).

L'après-midi de la Commission d'Étude du 15 mars 2018 sera consacrée à une présentation plus détaillée du RGDP, par Madame TRACOL et Maître TREHIOU, avocat spécialisé, qui pourront répondre à vos questions. ■