JOURNÉE D'ÉTUDE DU 15 MARS 2018

Le RGPD et ses applications en SSTI

Retour sur l'intervention de Mme Aurélie Tracol et de Me Erwan Trehiou sur le Règlement Général sur la Protection des Données, à retrouver en ligne dans son intégralité.

Applicable à compter du 25 mai prochain, le Règlement Général sur la Protection des Données (RGPD) concernera directement les SSTI. Ses grands principes (responsabilisation, coresponsabilité des sous-traitants, protection de la vie privée dès la conception, nouveaux droits des personnes…) ont été exposés dans le dernier numéro des Informations Mensuelles (n° 69, Mars 2018, pages 12 et 13), dans les suites d'une intervention de Mme Tracol, responsable de la sécurité des données chez AXESS solutions Santé, devant la Commission Système d'Information. On renverra à cet article ainsi qu'au support de présentation pour les définitions et principes de base du RGPD.

Accompagnée de Me Trehiou, avocat spécialisé, Mme Tracol est revenue sur ces principes, ainsi que sur leurs applications en SSTI (personnels concernés, mise en conformité…), lors de la réunion d'information du 15 mars dernier. En fin de support, 4 sujets font l'objet de focus détaillés : le sous-traitant, la gestion de la conformité des contrats, la garantie du *Privacy By Design* et l'analyse d'impact sur la protection des données.

Ressources :

À retrouver sur www.presanse.fr ▸ Espace adhérents :

- L'article « Applications du RGPD en SSTI (Archives ▸ Informations Mensuelles ▸ Base de données Articles)
- Le support de présentation de Mme Tracol et Me Trehiou (Présanse et ses instances ▸ Instances et organisations ▸ CSI

Applications du RGPD en SSTI

La prise en compte du RGPD, qui s'applique aussi bien aux données informatiques que papier et vise à renforcer à la fois le droit des personnes et la responsabilisation des entités, concerne par nature l'ensemble du SSTI : équipes Santé-Travail, services RH, relation adhérent, comptabilité, techniques, juridiques, communication… Cette mise en conformité telle qu'organisée par la CNIL (Commission Nationale Informatique et Libertés) comprend 6 étapes :

1 / Désigner un pilote : traitant à grande échelle des données sensibles, les SSTI ont l'obligation de nommer un Délégué à la Protection des Données (DPO, pour Data Protection Officer). Celui-ci peut être externe à la structure et mutualisé entre plusieurs Services. Son rôle est, entre autres, d'informer et conseiller le responsable de traitement ou le sous-traitant, de s'assurer du respect du RGPD et du droit national sur la protection des données. Le DPO est également le point de contact entre le SSTI et l'autorité de contrôle, avec laquelle il coopère.

2/ Cartographier le traitement de données personnelles : il s'agit de tenir un registre des traitements pour pouvoir être toujours en mesure de savoir qui traite les données, quelles sont les catégories de données traitées (données de Santé, autres), la finalité des traitements (dossier Santé-Travail, gestion RH), le lieu de stockage, la durée de conservation et les mesures de sécurité existantes.

3/ Prioriser les actions : un travail d'identification et de priorisation, pour chaque traitement, des actions de mise en conformité, au regard des risques pesant sur les personnes concernées. Exemples d'actions : minimisation (suppression des

données non indispensables à la finalité du traitement), identification d'une base juridique (consentement, contrat, obligation légale…) définition des modalités d'exercice des droits des personnes (droit d'accès, de rectification, portabilité…)…

4/ Gérer les risques : réaliser une analyse d'impact sur la vie privée contenant une description du traitement et de ses finalités, une évaluation de sa nécessité, une appréciation des risques et les mesures envisagées pour être conforme.

5/ Organiser les processus : il s'agit de mettre en place des processus internes précis pour une protection permanente des données : prendre en compte la question dès la conception d'une nouvelle application ou d'un nouveau traitement, sensibiliser la remontée d'information, définir les acteurs et les modalités…

6/ Documenter la conformité : si elle relève de l'obligation de moyens et non de résultats, la conformité du SSTI au RGPD doit pouvoir être prouvée à tout moment. Il faut alors avoir documenté les traitements de données (méthode, finalité, analyse d'impact sur la vie privée), l'information des personnes concernées (mentions d'information, modèles de recueil du consentement, procédures mises en place pour l'exercice de leurs droits…), ainsi que les contrats et responsabilités des acteurs.

Conclusion

Le RGPD représente un pas vers plus de protection des données personnelles et renforce ainsi la position des SSTI comme tiers de confiance. Outre le respect de la transition en 6 étapes décrites ci-dessus, la mise en conformité sera réussie aux conditions d'une communication claire et d'une sensibilisation de tous les collaborateurs à la démarche, et d'un suivi dans le temps avec une volonté d'amélioration continue. ■

Contrôle de l'application du RGDP par la CNIL

A noter que la CNIL a indiqué le 19 février dernier sur son site internet qu'elle fera preuve de souplesse dans le contrôle de l'application du nouveau RGPD pour les entreprises qui ne seraient pas prêtes pour son entrée en vigueur le 25 mai. Cette souplesse ne s'appliquera que pour les nouvelles obligations induites par le RGPD.

A toutes fins utiles, le lien suivant peut être consulté : **https://www.cnil.fr/fr/rgpd-comment-la-cnil-vous-accompagne-dans-cette-periode-transitoire**

A noter également qu'un accompagnement spécifique des délégués à la protection des données personnelles (PPO) concernant le volet « portabilité des droits » sera mis en place. La CNIL mettra aussi à disposition des outils pratiques, comme le logiciel PIA, qui facilite la réalisation des analyses d'impact sur la protection des données, ou encore un modèle de registre. Seront également mis en ligne prochainement des modèles types de mentions d'information, de formulaire de recueil du consentement et un formulaire de désignation du délégué à la protection des données.

Enfin, la CNIL élabore, en partenariat avec la Banque publique d'investissement (BPI), un guide spécialement conçu pour les TPE-PME. Elle organisera, en outre, des ateliers de sensibilisation et sectorielle au RGPD (santé, finance, technologie, etc.) et développera une offre de services et d'accompagnement dédiée à ces structures.

AGENDA

Du 19 au 20 avril 2018
Assemblée générale de Présanse
Reims

24 avril 2018
Assises du Maintien en Emploi
Paris

17 mai 2018
Ateliers de Présanse
Périgueux

Du 5 au 9 juin 2018
Congrès National de Santé au Travail
Marseille