RGPD : Ce qui va changer pour les professionnels de santé

	RGPD : Ce qui va changer pour les professionnels de santé

Fin des déclarations Cnil, demandes de consentement et sanctions renforcées, une nouvelle réglementation européenne* va venir chambouler la gestion des données personnelles en magasin. En tant que commerçants et professionnels de santé, vous collectez et transmettez des données relatives à vos clients. Le GDPR (General Data Protection Régulation) devra donc s'appliquer à votre point de vente. Zoom sur ce qui change dès le 25 mai 2018.

Registre des traitements et désignation d'un délégué à la protection des données

Quotidiennement vous gérez, stockez et envoyez les données de santé de vos clients que ce soit pour la pratique du tiers payant ou effectuer une commande auprès de vos fournisseurs. Identité, numéro de Sécurité sociale, facturation, prescription… vous êtes amenés à traiter des données personnelles, qui doivent actuellement faire l'objet d'une déclaration auprès de la Cnil (Commission nationale de l'informatique et des libertés). Mais bientôt, vous n'aurez plus besoin de cette formalité préalable.

En effet, le règlement européen sur la protection des données personnelles repose sur une logique de conformité, dont les acteurs seront désormais responsables. En d'autres termes, le poids de la procédure administrative va être transféré de la Cnil. **Dès le 25 mai 2018, vous devrez être en possession et tenir un « registre des traitements mis en œuvre ».** Ce dernier devra notamment spécifier :

• les catégories de données traitées ;
• la finalité ;
• les différents destinataires ;
• la durée de conservation.

« Ce registre informatisé permettra au professionnel de se ménager des preuves vis-à-vis de la Cnil. Il prouve son adhésion à un code de conduite, explique Maître Cécile Vernudachi, avocate au Barreau de Paris. Les grandes enseignes pourront également désigner un délégué à la protection des données, qui deviendra le point de contact avec la Cnil et un véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Dans les plus petites structures, ce ne sera pas une obligation », précise-t-elle.

Consentement renforcé et transparence

Le règlement européen impose également la mise à disposition d'une information claire, intelligible et aisément accessible à vos clients. Il définit en ce sens l'expression du consentement : « **les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer.** La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe », précise le document.

En d'autres termes, avant chaque devis ou chaque vente, vous êtes tenus d'obtenir le consentement de votre porteur pour pouvoir traiter et transmettre ses données personnelles. « Concernant la correction, seul le patient peut donner son accord pour la transmission de cette donnée, souligne Maître Vernudachi. **Son consentement doit obligatoirement être écrit.** Dans le cadre de l'exécution d'un contrat, il n'y a alors plus de restriction. Toutefois, il est interdit d'utiliser cette information pour la vendre à un tiers ou à des fins marketings et commerciales ».

Spécificité pour les moins de 16 ans :

Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Des sanctions encadrées et graduées

Les responsables de traitement, autrement dit les dirigeants ou chef d'entreprise, les plateformes de services et les complémentaires santé, peuvent enfin faire l'objet de **sanctions administratives importantes en cas de non-conformité au nouveau règlement**. Les autorités de protection peuvent notamment :

• prononcer un avertissement ;
• mettre en demeure l'entreprise ;
• limiter temporairement ou définitivement un traitement ;
• suspendre les flux de données ;
• ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
• ordonner la rectification, la limitation ou l'effacement des données.

S'agissant des amendes dans le cas d'une entreprise, elles peuvent s'élever de 2% à 4% du chiffre d'affaires annuel mondial, en fonction de la catégorie de l'infraction.

Notons que selon l'étude « Crossing the Line » du cabinet KPMG**, les Français sont 2ème sur le podium des consommateurs les plus vigilants quant au traitement de leurs données personnelles. Aussi, le règlement européen sera en vigueur dès le 25 mai 2018. Il vous faut donc être vigilant et vous y préparer dès maintenant !

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
****étude publiée en novembre 2016***

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Ce qui va changer dans les magasins pour le traitement des données personnelles | Acuité*