La Tribune de l'assurance

optimind.
manage risk, build your future

Conformité RGPD : les défis de la rentrée

Alors que le règlement général de l'Union européenne sur la protection des données (RGPD), adopté le 14 avril 2016, est applicable depuis mai 2018, les entreprises peinent encore à se conformer pleinement à cette nouvelle réglementation, tant les transformations qu'elle engage sont profondes.
Le législateur européen souhaite redonner aux citoyens le contrôle de leurs données personnelles, tout en assurant un cadre de protection des données solide et plus cohérent dans toute l'Union européenne (1), là où la directive européenne de 1995 avait échoué.
Pour bien comprendre les problématiques opérationnelles que rencontrent aujourd'hui les entreprises dans la mise en œuvre du règlement, il est important de rappeler quels sont les objectifs d'un tel texte législatif :susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur ; assurer aux personnes physiques la maîtrise des données qu'ils communiquent les concernant ; garantir la sécurité juridique et la transparence aux opérateurs économiques, y compris les micros, petites et moyennes entreprises, aux personnes physiques et aux autorités publiques. Le règlement entend ainsi renforcer les obligations applicables aux organismes publics et privés en matière de gouvernance et de sécurité des données à caractère personnel.
Les principaux apports du règlement : La notion de données à caractère personnel est élargie : données génétiques, données biométriques, adresse IP, etc. De nouvelles pratiques technologiques sont réglementées : le profilage, la pseudonymisation, etc.
La responsabilité du responsable de traitement est renforcée : il devra être en mesure de démontrer le bon respect des obligations qui lui incombe (renversement de la charge de la preuve) et apporter la garantie que les politiques relatives à la vie privée soient expliquées dans un langage clair et compréhensible. Le sous-traitant peut être tout aussi responsable que le responsable de traitement
Les droits des personnes sont modifiés. Certains droits sont renforcés (droit à l'effacement des données, droit d'être informé en cas de divulgation des données) d'autres sont nouveaux, comme le droit de transférer ses droits vers un autre fournisseur de données (droit à la portabilité des données). Des principes de gouvernance des données sont renforcés : transparence, limitation du traitement, le consentement recueilli doit être clair et explicite, minimisation des données ; privacy by default, privacy by design. La désignation d'un délégué à la protection des données (DPD) est obligatoire pour certains organismes publics ou privés (art. 37 et suivants).
Une étude d'impact relative à la protection des données est obligatoire en particulier pour les cas visés par l'article 35 du règlement. L'obligation de notification de violation des données ; Une consultation préalable de la Cnil est requise pour les traitements susceptibles d'engendrer un risque élevé. Un nouveau dispositif de coopération et d'échanges entre autorités de contrôles instaurant le mécanisme du guichet unique. Le renforcement des sanctions pouvant aller jusqu'à 4 % du chiffre d'affaires mondial pour une entreprise. Ces nouvelles obligations entraînent de profonds changements en matière de collecte des données personnelles, de traitement de ces données et de responsabilité des acteurs concernés. Des changements qui ont un impact global sur le fonctionnement des entreprises. En effet, certains nouveaux aspects du règlement se révèlent problématiques pour les entreprises et tout particulièrement pour les assureurs qui doivent protéger la donnée de santé, garantir la conformité du dispositif de protection des données personnelles mis en place et maîtriser le risque d'image et de réputation. Ils se doivent également de donner un cadre de sécurité solide des informations les plus sensibles ou critiques, telle que les données de santé dont l'utilisation du NIR (2) et disposer d'une infrastructure évolutive et adaptée aux nouvelles pratiques technologiques.

Si la plupart des entreprises ont entrepris leur projet de mise en conformité RGPD, l'analyse des impacts de ce nouveau règlement met en évidence un certain nombre de problèmes techniques et/ou opérationnels. En voici quelques-uns qui témoignent de l'ampleur du défi à relever :
Recensement des traitements

Si la Cnil rappelle clairement dans son guide intitulé « règlement européen sur la protection des données personnelles, se préparer en 6 étapes » (3) que pour mesurer concrètement l'impact du règlement européen sur la protection des données, il convient de recenser de façon précise les traitements de données personnelles mis en œuvre. Cette étape n'est pas aisée et reste source de difficultés pour les entreprises qui y sont confrontées. Pré-requis indispensable dans un projet de mise en conformité RGPD, le recensement des traitements implique de bien connaître son organisation,

son fonctionnement, ses activités et son maillage interentreprises.

La difficulté est double dans cet exercice. Non seulement, il faut cartographier ses traitements pour en avoir une vision globale, mais aussi en établir une identification précise, un à un. Une véritable fiche d'identité du traitement doit être établie.

Cette introspection viscérale de l'entreprise implique des moyens forts à déployer, l'engagement et la disponibilité des ressources concernées car l'exercice peut parfois être long, ainsi que le recours à des moyens techniques de localisation des données.

Responsabilité RGPD

Nous le savons, le règlement européen consacre une logique de responsabilisation de tous les acteurs impliqués dans le traitement des données personnelles, dès lors qu'elles concernent des résidents européens, que ces acteurs soient ou non établis au sein de l'Union européenne. Il entérine ainsi la notion de responsabilité du responsable de traitement, la notion de co-responsabilités entre plusieurs responsables de traitement et érige celle de responsabilité du sous-traitant (4).

Dans tous les cas, la difficulté pour les entreprises est dans un premier temps d'identifier les relations avec les tiers dans le cadre desquelles des données personnelles sont manipulées et dans un second temps, définir le statut RGPD de chaque partie prenante au contrat.

En matière d'assurance, cette analyse juridique n'est pas évidente tant il existe plusieurs typologies d'organismes d'assurance. Rappelons-le, ici, cette notion regroupe les entreprises d'assurance (sociétés anonymes d'assurance, sociétés d'assurance mutuelle, mutuelles et institutions de prévoyance), les entreprises de capitalisation, de réassurance, d'assistance et les intermédiaires d'assurance (agents généraux et courtiers d'assurance). Dans le cadre des autorisations uniques relatives au NIR et aux données d'infractions, de condamnations et mesures de sûretés, l'Agira (5) est également responsable de traitement.
Concrètement, il s'agit de préciser dans le contrat, le statut RGPD des parties au contrat et d'indiquer les obligations leur incombant pour protéger la sécurité et la confidentialité des données.
Cet exercice soulève parfois des difficultés quant à la détermination du statut RGPD et se traduit dans certains cas par une longue période d'échanges et de négociation entre les parties.

Au-delà de ces principaux défis, à la fois techniques et juridiques, les entreprises vont être confrontées dans les années à venir à d'autres problématiques du RGPD ; à ce titre nous pouvons citer la difficulté que rencontrent les acteurs dans la mise en œuvre concrète des droits des personnes, dont le droit d'accès : Comment donner accès ? À quoi ? Et à qui très précisément ? Autant de questions pratiques qui nécessitent études et travail en équipe, entre les métiers et l'IT.On peut également citer la détermination du fondement légal de certains traitements, ou encore le recueil du consentement, des obligations qui s'imposent aux entreprises, et qui pour autant ne sont pas une évidence, lorsqu'il s'agit de les décliner et de les mettre en œuvre. Sans oublier le déploiement des BCR (6), un vrai casse-tête pour les groupes qui souhaitent développer une gouvernance globale de la donnée personnelle, applicable à l'ensemble du Groupe.
Pour conclure, il est à noter que la Cnil a déjà réalisé un réel accompagnement auprès des entreprises et des acteurs de la place (guide, conseil…) qui ont cruellement besoin de solutions pratiques, concrètes et faciles à appliquer pour se conformer au RGPD, on ne peut que s'en féliciter.L'entrée en vigueur du règlement ne marque pas l'achèvement des travaux de conformité aux RGPD. Bien au contraire, une nouvelle génération de la protection des données est née et le règlement n'en est que l'ébauche. Les entreprises doivent encore relever les défis qu'il lance pour les années à venir.(1) considérant n°13 du règlement (UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016.(2) numéro de Sécurité sociale «NIR» (AU n° 31).(3)

https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf(4) articles 28, 30.2 et 37 du règlement européen sur les obligations du sous-traitant.(5) Association pour la gestion des informations sur le risque en assurance.(6) Binding Corporate Rules.
https://www.cnil.fr/fr/les-bcr-regles-internes-dentreprise