GESTION / FINANCE

Les Essentiels/Plus

Appliquer le RGPD dans l'assurance

Nordine Benhatta • Hugues Chamba

2e édition

L'ARGUS de l'assurance ÉDITIONS

Sommaire

7. Le RGPD, son contrôle et son application

Les enjeux de la mise en conformité pour les assureurs

1. Les enjeux de la mise en conformité au RGPD

1.1 La mise en œuvre opérationnelle du règlement

▶ Compréhension des enjeux

La prise de connaissance fine de l'esprit général d'une réglementation, quelle qu'elle soit, de ses règles spécifiques (nouveaux droits, nouvelles obligations), des risques encourus (amendes), des délais (dates d'entrée en vigueur), des outils suggérés ou mis à disposition par les textes, est indispensable pour aborder sa mise en œuvre. La mauvaise compréhension des enjeux peut avoir de nombreuses conséquences, comme le fait de sous-estimer l'impact d'une évolution réglementaire ou d'exposer la structure à des risques juridiques.

▶ Stratégie de mise en œuvre

Nous sommes à présent à un stade dans lequel l'essentiel, pour ne pas dire tous les organismes d'assurance, de courtage, de délégation de gestion ont entamé ou achevé la mise en conformité au RGPD. Les questions ne portent plus tant sur l'initiation du projet, puisque des actions ont déjà été menées, que sur le maintien dans la continuité, et l'adaptation ou amélioration de ce qui a été fait.

Comme lors des phases initiales de mise en conformité, des questions de stratégie de mise en œuvre se posent. Quelle ligne adopter (minimaliste ou plus complète), quels budgets consacrer, quelle priorisation et articulation avec les autres projets en cours, etc. ? Ces décisions relèvent du pilotage de la conformité et de la gestion du risque, notions communes à la gestion du risque cyber que nous allons voir plus loin dans le chapitre.

Pour être claires et légitimes auprès des équipes, la stratégie et les décisions qui en découlent doivent être prises par un organe dédié, et bien communiquée aux équipes.

▶ Diagnostic de conformité

En phase de mise en conformité initiale, la réalisation d'un « diagnostic de conformité » était indispensable pour permettre d'identifier, de définir, de planifier et de chiffrer les actions et investissements de mise en conformité.

Cette démarche est aussi utile, pour ne pas dire indispensable, pour le maintien dans la durée où pour une évaluation intermédiaire de la conformité d'une organisation au RGPD. Elle sert de socle pour répondre aux questions « Où en sommes-nous ? », « Qu'est-ce qui ne fonctionne pas ? », « Sur quoi sommes-nous en risque ? ».

Il est donc nécessaire de mettre à jour les documents qui ont été éventuellement réalisés initialement, ou à défaut de les produire.

▶ Plan de mise en conformité

Le diagnostic ayant permis d'identifier ou de mettre à jour les écarts entre la réalité et la conformité jugée acceptable, il est à présent nécessaire de définir la manière dont ces écarts doivent être rectifiés, quelle que soit leur nature.

Les points à traiter doivent être regroupés dans un plan de mise en conformité pour en maîtriser la cohérence par rapport à la stratégie définie. Cette étape n'est autre que la liste de tout ce qui devra être réalisé globalement pour la mise en conformité. Ces travaux ne peuvent atteindre leur but que s'ils sont adaptés et bien mis en œuvre. Ce plan de mise en conformité n'est en aucun cas assimilable à un plan d'action, qui serait beaucoup trop précis à ce stade et ne permettrait pas de disposer de la vue d'ensemble indispensable pour une bonne priorisation.

CAS PRATIQUE

Quels sont les travaux nécessaires pour le maintien ou l'amélioration de la conformité ?

Exemple : la finalisation de la mise à jour des contrats des sous-traitants, l'évaluation de l'exercice des droits d'information reçus par les clients ou les adhérents, le recensement des mesures actuelles de sécurité des données, la mise à jour de la cartographie des cycles des données à caractère personnel…

Quelle est la priorisation (coût, complexité, « Quick Wins »...) de ces travaux ?

▶ Plan de mise en œuvre

Le plan de mise en œuvre finalisé doit ensuite être décliné dans un plan d'action cohérent en termes de planning, de charges et de compétences. Un plan approprié de mise en conformité sera inutile si sa mise en œuvre est déficiente. L'efficacité est le maître mot pour les travaux de mise ou de maintien en conformité puisque parfois, ces travaux n'apportent pas de grande valeur ajoutée (commerciale, financière…) pour l'entreprise. Il est notamment utile de prévoir :
- l'organisation des chantiers ;
- la planification et les chiffrages ;
- la liste de tâches ;
- la mise en place de l'organisation projet ;
- le suivi et la maîtrise.

▶ Vérifications et contrôles

Compte tenu des enjeux et des risques encourus, il est nécessaire d'évaluer et de tester la conformité régulièrement. Le RGPD en est une illustration puisque la conformité sera évaluée par la CNIL au moment d'un éventuel contrôle. Le maintien de la conformité doit donc être prévu et organisé. Des contrôles réguliers seront mis en place pour s'assurer de la continuité, de la pertinence et de la qualité de la mise en conformité avec une activité de l'entité qui évolue au fil du temps. Cette étape est souvent sous-estimée et il arrive que des entreprises soient sanctionnées pour des failles techniques qu'elles pensaient pourtant sous contrôle. L'absence de suivi peut conduire à un effet tunnel avec des résultats ne correspondant pas aux exigences des auditeurs au moment précis d'un contrôle, ou au constat d'avoir mené des travaux inutiles. Aussi est-il nécessaire de :
- faire « vivre » les livrables et les process ;
- tester l'efficacité des mesures mises en place ;
- se préparer à d'éventuels contrôles.

▶ Les outils de la CNIL

La CNIL propose un ensemble de documents, d'outils et de recommandations pour faciliter l'application du règlement. Sans avoir force de loi, ces éléments sont à la fois des aides et des indications sur l'approche et l'interprétation qui seront faites des différentes dispositions du RGPD. S'appuyer sur ces travaux constitue naturellement un atout puisqu'ils favoriseront des gains de temps et garantiront à l'assureur une convergence de vision avec la CNIL sur l'application opérationnelle du règlement.

Les travaux du CEPD (Comité européen de la protection des données) constituent par ailleurs un éclairage précieux dans l'interprétation qui doit être faite d'un certain nombre de points.

Les outils et documents mis à disposition par la CNIL sur le sujet du RGPD pour l'ensemble des secteurs, mais aussi pour les assureurs, s'est bien étoffé ces deux dernières années.

▶ Outil Analyse d'impacts

La CNIL tient à disposition depuis 2018 un outil open source pour aider à faire les analyses d'impacts de l'article 35 du RGPD. Cet outil s'est régulièrement enrichi de retours terrains, et son ergonomie a largement progressé.

Il est à noter aussi que la liste des situations pour lesquelles ces analyses d'impacts a elle aussi été précisée, notamment après consultation par la CNIL du CEPD (Comité européen de la protection des données) pour préciser les cas d'exemption de cette obligation.

▶ Les packs sectoriels

Il s'agit d'un élément déterminant à prendre en considération dans la mise en conformité au RGPD pour les assureurs.

La CNIL présente les packs sectoriels de la façon suivante : « Élaborés en concertation avec les acteurs d'un secteur d'activité, les packs représentent un nouveau mode de régulation pour la CNIL. Ils visent à définir et diffuser les bonnes pratiques pour un secteur, tout en simplifiant les formalités administratives des acteurs qui s'y conforment. Ils peuvent ainsi contenir des mesures de simplification des formalités, des guides pratiques et pédagogiques, des tests de vérification de conformité à la loi. » (https://www.cnil.fr/fr/packs-de-conformite)

En juillet 2021, un guide actualisant les principes inscrits dans le pack de conformité assurance a été publié. Il a été élaboré en association avec la CNIL par le CTIP, France Assureurs, Planète CSCA et la Mutualité française (https://www.cnil.fr/fr/assurance). Il traite les thèmes suivants :

- qualification des acteurs du secteur de l'assurance au regard du RGPD ;
- finalités et bases légales des traitements ;
- profilage et décisions individuelles automatisées ;
- catégorie de données à caractère personnel traitées ;
- traitement du NIR ;
- traitement des données de santé ;
- informations des personnes concernées ;
- droits des personnes concernées ;
- destinataires ;
- durées de conservation ;
- mesures de sécurité.

▶ Des conseils sur la gestion du risque cyber

Ce point est développé dans la suite de ce chapitre, mais la CNIL a bien renforcé ses recommandations sur ce sujet spécifique, considéré à juste titre comme l'un des risques majeurs à prendre en compte.

1.2 Les pièges du maintien de la conformité dans le temps

Une fois le dispositif pour se mettre en conformité avec le RGPD mis en place, tout l'enjeu réside dans la capacité à maintenir ce niveau de conformité dans le temps et cette démarche reste exigeante.

Un maintien de la conformité dans le temps va s'appuyer sur plusieurs facteurs et notamment :

- analyser rigoureusement tous les nouveaux traitements de données personnelles et tous les traitements ayant fait l'objet de modifications ;
- apporter une attention particulière à l'exercice des droits des personnes concernées et à la sécurité des données ;
- mettre en pratique les process et procédures formalisées au moment de la mise en place du dispositif,
- s'efforcer de documenter au maximum ;
- organiser un échange régulier entre le responsable de traitement et le DPO qui reste un acteur essentiel dans ce cadre ;
- organiser une revue annuelle de la conformité.

Au-delà de la protection des données personnelles des personnes concernées, raison d'être du règlement, l'objectif est de disposer à tout moment d'un dispositif conforme et notamment en cas de contrôle de la CNIL. En en cas d'irrégularités les conséquences réputationnelles et financières peuvent être importantes.

De manière générale, les contrôles font souvent suite à des plaintes ou à des déclarations de violation de données. Les plaintes émanent généralement de particuliers mécontents de sollicitations non souhaitées, d'une anomalie constatée dans un espace en ligne, de la non-réponse à leur demande d'exercice de l'un des droits décrits précédemment dans l'ouvrage.

La bonne préparation à d'éventuels contrôles de la CNIL est un objectif tout aussi important, dans le sens où cette dernière est missionnée pour s'assurer de la bonne application du règlement et peut prononcer des sanctions.

La documentation, le respect de l'information des personnes concernées, la formalisation des actions mises en place prennent alors toute leur importance.

Penser que la sécurité serait assurée uniquement par l'existence d'un registre des activités de traitement bien tenu serait naïf. Considérer qu'un système d'information régulièrement testé via des tests d'intrusion suffira à contenter la CNIL le serait tout autant. Une autorité de contrôle veillera surtout à la réalité opérationnelle des actions, à leur pertinence, à leur efficacité.

Appliquer le RGPD dans l'assurance

Nordine Benhatta

Avocat au barreau de Paris et associé fondateur du cabinet B2N Avocat, membre du réseau Lautrette et Associés, il exerce une activité de conseil et de défense. Il accompagne les acteurs du marché de l'assurance en matière de gouvernance, conception/distribution de produits d'assurance, protection des données personnelles, avec une expertise notable en droit de la mutualité. Il a participé à de nombreux projets de mise en conformité au RGPD.

Hugues Chamba

Issu d'une double formation juridique et école de commerce, il a été associé du groupe Valmen pendant plusieurs années, coordonnant des missions d'aide à la prise de décision et de transformation. Il a accompagné de nombreuses entreprises sur la mise en conformité au RGPD avant d'élargir ses interventions au domaine de la cybersécurité.

Depuis le 25 mai 2018, le Règlement général sur la protection des données (RGPD) est entré en vigueur, complété en France par des dispositions législatives spécifiques. Dans un contexte de développement toujours grandissant des nouvelles technologies et de l'informatique, les données à caractère personnel, au cœur des enjeux économiques mondiaux, font désormais l'objet d'une protection renforcée. Ce niveau d'exigence pour les responsables de traitement et les sous-traitants génère des contraintes supplémentaires pour les assureurs et leurs partenaires collectant ces données.

L'objectif de cet ouvrage est d'exposer les grandes lignes du RGPD (de l'historique au pilotage et aux enjeux de la mise en conformité) et, au-delà, de rendre compte des problématiques rencontrées par les professionnels de l'assurance dans l'application et surtout le maintien dans le temps de ces règles. Il intègre un zoom sur les précisions opérationnelles apportées par les instances nationale et européenne (CNIL et CEPD), ainsi que sur les sanctions qui ont déjà été prononcées.

Enfin, cette nouvelle édition s'enrichit de développements consacrés à la cybersécurité, sujet étroitement imbriqué au RGPD et que l'actualité a plus que jamais porté en tête des priorités des assureurs.

ISBN 978-2-35474-400-7

Les Essentiels/Plus