Livre blanc

Se préparer au RGPD / GPDR : résultats OCC 2018

L'heure de la mise en conformité avec le RGPD / GPDR (Règlement général sur la protection des données) a sonné. Une stratégie RGPD / GDPR doit être mise en place pour limiter les risques de non-conformité, et atteindre les objectifs commerciaux à long terme tout en apportant une relation client de qualité.

Présentation

Pour aider les assureurs à avancer dans leur mise en conformité avec le RGPD / GDPR, One Connected Community (OCC), Microsoft et Hitachi Solutions se sont associés pour réunir un groupe de cadres dirigeants travaillant dans le domaine des assurances pour un atelier de réflexion au Gherkin de Londres. Les échanges ont porté sur les mesures pratiques que les compagnies d'assurance peuvent prendre pour réussir leur mise en conformité et exploiter les nombreuses opportunités offertes par le RGPD / GDPR.

Les résultats, fournis* directement par les professionnels du secteur de l'assurance, peuvent servir de référence aux compagnies d'assurance qui travaillent à leur mise en conformité avec le RGPD / GDPR depuis le 25 mai 2018.

Le rapport souligne que le RGPD / GDPR, s'il est bien mis en œuvre, peut permettre de renforcer la relation client. Mais pour y parvenir, les assureurs doivent établir de nouvelles normes en matière de confidentialité des données.

Mettre de l'ordre dans ses données

78 %

...de nos assureurs ont mené un audit pour cartographier leurs flux de données

Le RGPD / GPDR incite les compagnies d'assurance à mieux maîtriser leurs données et à les exploiter le plus efficacement possible, à travers les multiples fonctions de leurs activités.

Comme l'exprime Udo Pickartz, Directeur de la conformité UE chez Starstone Insurance : « De nombreuses parties du RGPD / GDPR étaient déjà couvertes par les précédents principes de protection des données.

À propos de l'étude : Cette étude a été menée par One Connected Community en partenariat avec Hitachi Solutions Europe entre septembre 2017 et mars 2018. Ont participé des cadres dirigeants de : Wesleyan, Swiss Re, OBE, Enstar Group, Aspen Insurance Group, Canada Life, Hyperion Insurance Group, LV, Starstone Insurance, Munich Re, Brit Insurance, Covea Insurance. One Connected Community souhaiterait remercier tous les participants pour le temps consacré et les idées partagées.

Pour autant, des éléments du RGPD / GPDR, comme l'augmentation du montant des amendes, ont contribué à l'amélioration de la gestion des données. Cette réglementation permet aux entreprises de prendre le contrôle des données en leur possession, ce qui, pour beaucoup, n'étaient jusque là pas encore maîtrisé. »

De plus, Andy Gill, Responsable du programme RGPD / GPDR chez Hitachi Solutions, constate que le coût de stockage des données est un autre facteur qui décide les compagnies d'assurance à mener un audit. Selon lui : « Historiquement, il n'y avait aucune raison économique de mettre de l'ordre dans ses données. Il était bien plus coûteux de re-cartographier toutes ses données que de simplement les conserver indéfiniment. Mais avec la prise en compte des éventuels coûts d'une non-conformité au RGPD / GPDR, l'aspect économique s'est renversé. Cela permet d'améliorer les politiques de conservation des données, la gestion de la documentation, la classification de l'information, etc. »

Il ne s'agit plus de faire face au coût du stockage des données, mais aux risques qui l'accompagnent. Étant donné que ce secteur, par sa nature même, traite de gros volumes de données, la conservation et la suppression des données constituent un aspect particulièrement problématique du RGPD / GPDR.

Le dilemme de la conservation des données

De tous les aspects du RGPD / GPDR, la conservation et la suppression des données est peut-être le plus complexe à gérer pour le secteur de l'assurance. Les compagnies d'assurance gèrent de gros volumes de données et de nombreux processus reposent sur l'acquisition de données dans la durée (et des renseignements qu'elles fournissent).

Il en résulte une réticence envers la suppression pure et simple des données. À la place, les compagnies d'assurance proposent une multitude de stratégies, de systèmes et d'approches qui permettent de se conformer à la loi tout en conservant les données lorsque cela est possible. Pour résumer, les grands objectifs du secteur (croissance et acquisition de nouveaux contrats) pourraient bien en pâtir si le RGPD / GPDR prive ce dernier d'un océan de données qui se sont accumulées au fil du temps.

Que conserver ? Que supprimer ?

Pour faire face au dilemme de la conservation des données, il est vital de bien comprendre l'importance d'avoir des ensembles de données différents, pour des processus métier variés. Par exemple, le droit fondamental à l'information sur les polices pourrait exiger une période de conservation des données relativement longue afin d'allonger les délais de déclaration des sinistres.

Adrian Dobrovicz, Architecte métier chez LV, explique : « Les différents secteurs de l'entreprise n'ont pas les mêmes exigences en matière de données. Ce que vous faites en amont en termes de conservation des données doit correspondre à l'utilisation que l'entreprise en fait en aval. »

28 %

...de nos assureurs disposent d'un processus pour éliminer les données à caractère personnel à la fin des délais légaux ou lorsqu'un individu exige leur suppression

Anonymisation

L'anonymisation et la pseudonymisation sont une solution pour éviter la suppression des données, selon Anwar Ahmed, Architecte solutions en chef chez Munich Re.

« En ce qui concerne la conservation des données, choisir l'anonymisation constitue une bonne alternative à la suppression. L'analyse des données s'améliore avec le temps et le fait de les conserver nous permet d'en tirer davantage de précieuses informations. Ceci étant dit, notre ligne de conduite doit viser à éviter de supprimer des données. »

L'anonymisation, bien sûr, consiste à transformer les données pour leur donner une forme non nominative. Mais étant donné qu'un individu peut être identifié par une référence à un identifiant tel qu'un numéro de carte d'identité ou des données de localisation, il est difficile de garantir une anonymisation à 100 % des données.

L'anonymisation exige de chaque compagnie d'assurance qu'elle évalue les risques associés, en estimant à quel point l'anonymisation peut alléger le fardeau de la mise en conformité au regard du risque qu'elle ne soit pas efficace à 100 %.

Cadre juridique

Tanya Jacobs, Responsable de la gestion des risques chez Hyperion Group, est favorable à une approche qui insiste sur le cadre juridique de la conservation des données.

« La stratégie en matière de conservation des données appelle une question simple : existe-t-il un motif légal ou réglementaire de conserver les données ? La conservation des données doit répondre à un besoin de l'entreprise et être dans le meilleur intérêt du client. »

55 %

...de nos assureurs ont identifié une base légale pour le traitement de leurs données

Transparence

Votre réponse au RGPD / GPDR sera satisfaisante si elle respecte la réglementation tout en créant de la valeur commerciale. Gagner la confiance de vos clients constitue une excellente occasion de créer de la valeur commerciale. Être transparent sur la façon dont vous utilisez les données de vos clients contribuera grandement à bâtir une relation de confiance avec eux.

Andy Gill, Responsable du programme RGPD / GPDR chez Hitachi Solutions, explique en quoi une gestion des données centrée sur les clients forme une opportunité extraordinaire. Selon lui : « Le consentement explicite et les déclarations de confidentialité créent un dialogue qui fait comprendre au client : "ce sont vos données, nous en prenons soin et nous les traitons avec le plus grand professionnalisme". »

C'est cette interaction qui permet d'instaurer la confiance. C'est donc sans surprise que seulement :

11 %

...de nos assureurs pensent que le RGPD / GPDR aura un effet négatif sur la commercialisation de leurs produits auprès de leurs clients

Au contraire, renforcer la transparence est un excellent moyen de cultiver des relations clients de meilleure qualité.

Droits des personnes concernées

Malgré les faibles volumes enregistrés par le passé, il est important de prendre en considération la possibilité d'une forte augmentation du nombre de demandes d'accès, en raison de la publicité faite autour du RGPD / GPDR.

« La publicité autour du RGPD / GPDR crée une "vitrine" pour l'exercice des droits des clients sur leurs données. Si l'entreprise n'a pas mis en place un processus pour traiter de telles demandes, sa réputation risque d'en souffrir », affirme Amanda Hurst, Directrice de la conformité chez Canada Life.

Ces demandes sont particulièrement difficiles à traiter pour les compagnies d'assurance avec une multiplicité d'anciens systèmes. Si une entreprise est perçue comme désorganisée et incapable de traiter les demandes, ce sont probablement les sociétés de gestion des sinistres qui en profiteront.

« Pour alléger le nombre de demandes d'accès par les personnes concernées, la transparence est fondamentale », explique Steve Jackson, Directeur de la répression de la criminalité financière chez Covea Insurance.

« La communication avec les clients doit démontrer à quel point vous êtes bons dans la gestion de leurs données. Vous pouvez ainsi tisser un lien de confiance avec vos clients, qui ne vous noieront pas sous les demandes d'accès », ajoute-t-il.

Ceci étant dit, la complexité du modèle de distribution des assurances implique que les demandes d'accès par les personnes concernées sont particulièrement difficiles à gérer d'un point de vue technique. Par exemple, bien que la plupart des assureurs puissent extraire les données à caractère personnel de leurs propres systèmes, l'on s'attend également à ce que le contrôleur des données soit aussi capable d'extraire ces données auprès des partenaires avec lesquels elles sont partagées.

Prouver sa conformité

Au-delà de la mise en œuvre de procédures de gestion des données conformes au RGPD / GPDR, les compagnies d'assurance ont l'obligation de documenter le traitement des données, les sauvegardes et les polices, et de tenir à jour leur documentation au fur et à mesure que les processus métier évoluent.

La tenue à jour d'une documentation précise risque de créer un important besoin en ressources supplémentaires, selon Udo Pickartz, Directeur de la conformité UE chez Starstone Insurance.

« Vous avez beau faire tout ce qu'il faut et prendre toutes les mesures nécessaires pour vous conformer au RGPD / GPDR, si vous n'avez pas documenté les preuves pour en attester, vous risquez des ennuis avec l'organisme de réglementation. Un système de conservation des preuves est crucial pour prouver sa conformité en continu », ajoute-t-il.

89 %

...de nos assureurs ont mis en place un système de détection et de signalement des violations de données

Stuart Riley, Directeur de la conformité chez Aspen Insurance Group, confirme que la conservation de preuves de conformité suffisantes est cruciale. Cependant, il soutient qu'insuffler une culture de la protection de la vie privée dès le départ est le plus grand défi à relever. Selon lui : « C'est une chose que de tenir à jour un historique des polices et des procédures, mais le véritable défi concerne la culture, c'est-à-dire combien de personnes respectent réellement ces procédures. »

En guise de test de vérité, les compagnies d'assurance devraient se demander : est-ce que je réussirais le test si l'organisme de réglementation évaluait la mise en œuvre pratique de nos polices et de nos procédures au jour le jour ?

Changement de culture

Avoir la bonne culture revêt une importance vitale, insiste Andy Gill, Responsable du programme RGPD / GPDR chez Hitachi Solutions.

« Vous avez beau disposer des meilleurs systèmes, des meilleurs processus et de la meilleure volonté du monde, il est impératif que cela se reflète dans les actes des personnes. Il s'agit d'un périple visant à éduquer les entreprises et à leur faire comprendre que les données appartiennent aux clients. Elles ne doivent être stockées que s'il existe un intérêt légitime à le faire.

Du point de vue de la réglementation, des problématiques telles que le stockage sur des appareils personnels et l'impression de documents peuvent aller à l'encontre de la conformité. Cependant, modifier ces processus n'est pas une mince affaire. Il faut changer les habitudes et les croyances de chacun », ajoute-t-il.

Preuve que le changement culturel est difficile, seulement :

33 %

...de nos assureurs ont la certitude que l'ensemble de leur personnel est pleinement conscient de l'importance de mieux gérer les données dans le cadre du RGPD / GPDR

Pour Hyperion Group, une des options consiste à verrouiller tout ce qui n'est pas connecté au réseau, selon la responsable de la gestion des risques, Tanya Jacobs.

« Une échéance inflexible pour que les collaborateurs transfèrent toutes leurs données sur le système autorisé devrait les inciter à s'adapter aux nouvelles pratiques et, espérons-le, nous épargner quelques soucis à long terme. L'astuce pour changer les habitudes, c'est de faire de la conformité la voie du moindre effort. »

Parmi les autres approches, Adrian Dobrovicz, Architecte métier chez LV, mentionne les permissions basées sur les rôles.

« Toutefois, la gestion des permissions basées sur les rôles est complexe. Par exemple, les transferts internes au sein d'une équipe se traduiront par des droits d'accès différents. Le défi consiste à faciliter la modification des permissions sans que cela devienne un énorme fardeau administratif », affirme-t-il.

Conclusions

Qu'il s'agisse de mettre en œuvre de nouveaux processus métier, d'intégrer de nouvelles technologies ou de documenter vos polices et vos procédures, il est important de maintenir un réel équilibre. Un équilibre qui garantisse votre conformité, sans jamais vous faire perdre de vue les grands objectifs de l'entreprise.

Selon Stuart Riley, Directeur de la conformité chez Aspen Insurance Group, le RGPD / GPDR est une question de gouvernance plus globale. « Le danger est de l'aborder simplement comme une liste de critères à remplir jusqu'à la fin du mois de mai. »

Si l'on reconnaît que la conformité et la croissance commerciale ne sont pas antinomiques mais vont de pair, on a la clé du succès. La conformité au RGPD / GPDR doit être mise en œuvre en cohérence avec le modèle commercial de l'entreprise.

Cela implique de définir des normes plus élevées pour la protection de la vie privée des clients. Ceux qui y parviendront deviendront les gardiens de confiance des données à caractère personnel, ce qui se traduira par des relations plus riches et pérennes avec les clients.

Il est crucial d'insuffler une culture de la protection de la vie privée dès le départ. Bien que le changement de culture soit une tâche difficile, il est nécessaire pour établir de meilleures normes en matière de gestion des données et de transparence - des normes que les clients exigent de plus en plus de leurs prestataires d'assurance.

En quoi Hitachi Solutions peut-il vous aider ?

Avez-vous du mal à gérer la complexité de vos nombreux systèmes ? Reconstituez-vous les informations de vos clients à partir de différentes données dont vous disposez ? Vos systèmes sont-ils dotés des fonctionnalités nécessaires pour recueillir le consentement explicite de vos clients ? Votre technologie permet-elle de répondre aux demandes d'accès des personnes concernées et de respecter le droit à la portabilité des données ?

En collaboration avec le secteur de l'assurance, Hitachi Solutions recherche des moyens innovants et efficaces de réunir différentes catégories d'informations. Hitachi Solutions accompagne votre mise en conformité avec le RGPD / GPDR et, en même temps, vous apporte une vision globale de vos clients. En unifiant une structure souvent cloisonnée, nos systèmes contribuent à éliminer les problèmes d'efficacité et à garantir votre conformité. Qu'il s'agisse de gestion des polices ou des sinistres, tout le travail d'Hitachi Solutions vise à améliorer vos processus, produire de la valeur ajoutée et fidéliser vos clients.

Contactez Hitachi Solutions pour en savoir plus : www.hitachi-solutions.fr/contact/

Hitachi Solutions

Microsoft | Dynamics 365