À PROPOS DE WYDE

Depuis sa création en 1997, Wyde, une entreprise Mphasis, est leader dans le monde de l'édition de progiciel d'assurance notamment au travers de Wynsure, son progiciel de gestion. Wyde jouit d'une présence internationale avec un siège à Bloomington aux États-Unis, des bureaux au Canada, un centre de Recherche et Développement à Paris et des centres d'excellence en Inde et en Pologne.

Wynsure est multi-langues, multi-devises et très configurable, ce qui permet une gestion simplifiée des contrats, des sinistres et de la facturation pour l'ensemble des produits du marché Prévoyance & Santé ainsi qu'Affinitaire. Wynsure peut être déployé pour une ou plusieurs lignes métiers, en solution globale ou par module.

Notre succès est le résultat de nos valeurs :

- Excellence de notre technologie et de notre expertise
- Solution centrée sur nos clients avec une anticipation des tendances du marché
- Investissement continu dans nos développements R&D
- Innovation et capacité de rapidement se renouveler pour répondre aux besoins du marché

ABOUT MPHASIS

Mphasis enables customers to reimagine their digital future by applying a unique formula of integrated cloud and cognitive technology. Mphasis $X2C^{2}_{TM}$ formula for success, (shift anything to cloud and power everything with cognitive), drives five dimensions of business value with an integrated consumer-centric Front to Back Digital Transformation, enabling Business Operations and Technology Transformation. Mphasis applies advancements in cognitive and cloud to traditional application and infrastructure services to bring much needed efficiency and cost effectiveness. Mphasis' core reference architectures and tools, combined with domain expertise and hyper specialization are the foundation for building strong relationships with marquee customers. Click here to know more.

For more information, log on to
www.wyde.com

www.wyde.com

VAS 04/12/17 A4 BASIL 4531

WYDE™
Nous facilitons la vie des Assureurs

Mphasis
Unleash the Next

WYDE™
Nous facilitons la vie des Assureurs

Assurance: comment passer sereinement au RGPD?

Meilleures pratiques métiers et SI pour une mise en conformité réussie

Droit de propriété intellectuelle : *Comment passer sereinement au RGPD. Meilleures pratiques métiers et SI pour une mise en conformité réussie est un ouvrage édité par Wyde (103/105, rue Anatole-France, 92 300 Levallois-Perret - www.wyde.com)*

Directeur de la publication : Philippe Payet (directeur général Wyde Europe)

Directeur éditorial : Baptiste Sevezen (directeur commercial Wyde France)

Rédaction en chef déléguée : Contenteo (contenteo.com)

Rédaction : Delphine Tissier

Remerciements à : Adèle Adam, Philippe Bouvier, Umberto d'Amico, Olivier Iteanu, Quang Nghiem, Clara Petit

SOMMAIRE

EXECUTIVE SUMMARY

Parmi les problématiques métiers du moment qui touchent le secteur de l'assurance, le Règlement général pour la protection des données (RGPD) ne manque pas d'être anxiogène ou tout du moins de poser question.

Entré en vigueur en 2016 et appliqué le 25 mai 2018 à toutes les entreprises et organisations qui collectent, traitent et stockent des données personnelles en Europe, le RGPD repose sur la protection des données personnelles. Cette nouvelle contrainte réglementaire entraine des impacts importants sur les entreprises aussi bien pour les métiers que la DSI.

Le RGPD vient renforcer les droits des assurés et les obligations des entreprises. C'est l'occasion pour elles de transformer leur approche de la gestion du cycle de vie des données, en saisissant toutes les opportunités pour marquer leur différence face à la concurrence.

Ce livre blanc est l'occasion pour Wyde de partager conseils et best practices pour un passage serein au RGPD.

ÉDITO

Le Règlement général pour la protection des données (RGPD) est une « Loi » majeure de l'Union européenne. C'est un changement inéluctable et exigeant. Son entrée en application le 25 mai 2018 bouleverse le rapport des compagnies d'assurance aux données qu'elles détiennent et à leurs clients.

Les données à caractère personnel sont au cœur du métier de l'assurance. Leur collecte et leur traitement portent non seulement sur une diversité de cibles (l'assuré lui-même, les collaborateurs de l'organisation ou encore des tierces personnes lors de sinistres), mais également sur une multiplicité d'informations, parfois sensibles (état de santé, identité des particuliers, coordonnées bancaires...). Leur exploitation nécessite donc la plus grande prudence. Le RGPD vient renforcer la protection de ces données, via le recueil d'un consentement explicite et fort des assurés, de nouveaux droits pour l'assuré comme les droits à l'oubli ou à la portabilité des données, ainsi qu'une information complète et détaillée sur les traitements mis en œuvre...

Les sociétés d'assurance n'ont d'autres choix que de s'adapter à ce nouvel environnement. Il leur faut nommer un Data Protection Officer (DPO) pour chapeauter la mise en conformité, s'assurer que sous-traitants et prestataires s'acquittent des mêmes obligations issues du RGPD ou encore établir une cartographie globale de l'ensemble des données détenues.

Ce livre blanc est l'occasion pour Wyde de partager conseils et meilleures pratiques pour un passage serein au RGPD.

Wyde, en tant qu'ESN (entreprise de services du numérique) et éditeur spécialisé, se propose d'accélérer la digitalisation pour le secteur de l'assurance. Dans ce contexte, la société propose ce livre blanc pour aborder plus sereinement le RGPD : pourquoi le métier d'assureur est-il directement impacté ? Comment le règlement transforme ce métier et sa relation avec le client ? Quelle est la checklist à définir pour prendre en compte les changements réglementaires au niveau des outils de gestion ?

Nous partageons également dans cet ouvrage nos best practices afin de mettre en valeur des conseils d'experts (des partenaires, des avocats, des spécialistes métiers) pour un passage au RGPD rassurant.

Bonne lecture !

Philippe Payet

Directeur Général Wyde Europe

ILS ONT DIT

Entré en vigueur en 2016, le RGPD est appliqué au 25 mai 2018 immédiatement dans tous les États membres de l'Union européenne. Le processus est irréversible car cette date figure dans le Règlement lui-même à son article 99. Le RGPD ne revêt pas seulement un risque financier au vu des lourdes sanctions, mais également un risque d'image pour tout contrevenantt.

Me Olivier ITEANU,
Avocat spécialiste du droit des technologies de l'information, Cabinet Iteanu Avocats

Mon cheval de bataille en tant que DPO est la chaine de sous-traitance, car il est important de comprendre que si un seul maillon n'est pas conforme ou ne met pas en place des mesures de sécurité, c'est toute la chaine qui est affaiblie.

Adèle ADAM,
DPO de Claranet

Les assureurs veulent de plus en plus capter de données : le RGPD permet de "tout" faire pourvu qu'on le fasse dans le respect des règles établies. Si on veut conserver un maximum de données, il suffit de les anonymiser pour ne plus remonter à leur propriétaire et de les archiver au fur et à mesure que les délais de conservation sont dépassés. C'est très nouveau, et cela va transformer le commerce, la gestion et la relation client.

Quang NGHIEM,
Conseiller chez Crysal

Notre rôle en tant qu'éditeur de logiciels est aussi de sensibiliser nos clients aux impacts du RGPD sur le métier d'assureur et de montrer que nous aussi nous y travaillons. Nous conseillons notamment d'anticiper la notion de portabilité des données.

Philippe BOUVIER,
Product Manager chez Wyde

« L'anonymisation a pour but d'empêcher irréversiblement l'identification directe ou indirecte de la personne concernée. Il ne s'agit alors plus d'une donnée personnelle. Cette mesure est à distinguer de la pseudonymisation, qui constitue un traitement au sens du RGPD, et qui permet de ne plus identifier une personne à un moment donné, mais avec un retour en arrière possible.

Me Clara PETIT,
Avocate spécialiste en données personnelles et e-réputation, Cabinet Iteanu Avocats

En tant qu'unique entité dédiée à l'assurance, RCI Malta doit gérer des problématiques spécifiques à ce secteur, avec notamment un projet pour identifier les besoins et les impacts sur les métiers. Nous avons démarré les travaux depuis mars 2017. Des ateliers de suivi, avec une documentation approfondie sur la mise en œuvre et l'évangélisation du sujet, sont organisés chaque mois avec les différentes entités de RCI Corporate.

Umberto D'AMICO,
IT Manager chez RCI Malta

PARTIE 1

QU'EST-CE QUE LE RGPD?

200 pages 99 articles

OBJECTIFS

- Redonner la maitrise des données personnelles aux personnes physiques
- Harmoniser les pratiques dans tous les États membres de l'Union européenne
- Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles
- Responsabiliser toute la chaine des acteurs traitant des données
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données

ORGANISMES CONCERNÉS

- Tous les organismes privés ou publics (responsables et sous-traitants) disposant d'un établissement sur le territoire de l'UE ou proposant des biens ou services aux citoyens de l'UE, ou observant le suivi du comportement de personnes physiques au sein de l'UE notamment sur internet

SANCTIONS

- Jusqu'à des amendes administratives de 20 millions d'euros ou d'un montant égal à 4 % du chiffre d'affaires annuel mondial total, notamment en cas de violation des principes de base d'un traitement, par exemple, en cas de transfert de données hors de l'UE sans respecter les règles établies par le RGPD ou en cas de non-respect du droit d'accès des personnes physiques
- Jusqu'à des amendes de 10 millions d'euros ou d'un montant égal à 2 % du chiffre d'affaires annuel mondial total, notamment en en cas de manquement aux obligations pouvant incomber au responsable de traitement et/ou au sous-traitant quant à l'établissement d'un registre des activités de traitement, d'une analyse d'impact, ou à la mise en place de mesures de sécurité ainsi que la notification d'une violation de données
- Droit à réparation du préjudice subi pour toute personne victime d'une violation de ses données personnelles, avec le cas échéant des actions de groupe

CONTRÔLE

- Les autorités de contrôle (la Commission nationale de l'informatique et des libertés CNIL pour la France) peuvent intervenir de manière inopinée et ordonner des contrôles réguliers du respect du Règlement en cas de première infraction involontaire. En principe, les entreprises contrôlées peuvent répondre et réagir aux reproches formulés par les autorités de contrôle en prenant un ensemble de mesures de mise en conformité

RGPD: Les Points Essentiels

Un nouveau règlement européen sur la protection des données

Aboutissement d'un long travail législatif entre les États-membres européens, débuté en 2012, le Règlement général sur la protection des données (RGPD), aussi connu sous le nom de General Data Protection Regulation (GDPR en anglais), entre en application le 25 mai 2018, dans toutes les entreprises qui collectent, traitent et stockent des données personnelles en Europe. Rappel des points essentiels à connaitre.

"Renforcer le contrôle des résidents européens quant à l'utilisation de leurs données personnelles."

Le RGPD a pour principal objectif de permettre aux personnes résidant dans l'Union européenne de bénéficier d'un contrôle renforcé sur l'utilisation par des tiers, organismes privés ou publics, de leurs données personnelles.

Il unifie le cadre juridique minimum pour l'ensemble des pays européens, et harmonise la réglementation pour les entreprises en matière de cybersécurité : elles doivent veiller à ce que ces données soient totalement sécurisées, en tout lieu et à tout moment, contre les risques de perte, de vol, de divulgation, d'accès non autorisé...

Sur un plan technique, le nouveau règlement vient non seulement pallier l'hétérogénéité de l'application de la précédente directive européenne de 1995 sur la protection des données, mais également renforcer le dispositif réglementaire pour mieux s'adapter à la révolution digitale, à l'explosion des données, leur recueil et leur exploitation.

Les conséquences sont très nombreuses et importantes. Parmi les changements les plus attendus pour les entreprises françaises:

- **l'obligation du responsable de traitement de notifier à la CNIL** *(Commission nationale de l'informatique et des libertés) dans les 72 heures de sa connaissance, un cas de violation des données, le sous-traitant doit quant à lui notifier toute violation de données au responsable de traitement « dans les meilleurs délais » après en avoir pris connaissance*
- **la mise en place d'un DPO** *(Data Protection Officer ou délégué à la protection des données en français), obligatoire en particulier en cas de suivi régulier et à grande échelle des personnes physiques, ou encore dans le cas d'un traitement de données dit à risque en raison par exemples du volume traité ou du type de données traitées. Les assurances devraient en principe désigner un DPO*
- le renforcement du **contrôle des sous-traitants,** désormais sousmis à la réglementation spécifique CNIL
- le droit à **la portabilité des données** qui permet à une personne de demander à son responsable de traitement de transférer ses données à un autre, par exemple en cas de changement de prestataire

- **l'obligation d'indiquer la durée de conservation des données,** les droits d'accès, de modification et de suppression (droit à l'oubli) de données, ou encore le droit pour une personne physique de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (y compris le profilage) produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Au vu des nouveaux pouvoirs de sanction accordés aux autorités nationales de régulation (la Commission nationale Liberté et Informatique en France, CNIL), soit 4% du chiffre d'affaires mondial annuel des entreprises (contre 150 000 euros en France jusqu'à une date récente[1]), les entreprises ont tout intérêt à avancer rapidement vers leur mise en conformité. Car, dès le 25 mai 2018, le RGPD introduit une logique de responsabilisation, c'est ce qu'on appelle le principe d'« Accountability » : tout responsable du traitement doit être en mesure de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données, et surtout, les prouver par une documentation.

L'avis de l'expert

« Entré en vigueur en 2016, le RGPD est directement appliqué au 25 mai 2018 et dans tous les États membres de l'Union européenne. Le processus est irréversible. Le RGPD ne revêt pas seulement un risque financier au vu des lourdes sanctions, mais également un risque d'image pour tout contrevenant. Il existe un réel avantage business à se mettre en conformité le plus rapidement possible. La nouveauté réside dans l'extension horizontale du règlement : les entreprises doivent à la fois l'appliquer et "contraindre" leurs sous-traitants et leurs partenaires à en faire de même pour ne pas risquer d'engager leur propre responsabilité. »

Maître Olivier Iteanu

Avocat spécialiste du droit des technologies de l'information - Cabinet Iteanu Avocats

Pourquoi les assureurs sont directement impactés ?

Les données personnelles au cœur du métier

Le secteur de l'assurance est en première ligne en ce qui concerne la protection des données personnelles. Avec le RGPD, il fait face à plusieurs défis : se mettre en conformité avec ce nouveau règlement, continuer de recueillir des données pour répondre aux attentes des assurés, rester en mesure de lancer de nouvelles offres toujours plus contextualisées.

Établir des devis, proposer une nouvelle couverture d'assurance ou des services financiers, gérer les sinistres, s'occuper de relations clients... Les assureurs manipulent quotidiennement des données personnelles, qu'elles soient dites à risques (coordonnées bancaires, numéro de sécurité sociale, données d'infraction et de condamnation et géolocalisation en temps réel) ou sensibles/particulières (santé, données biométriques...).

Données personnelles : une matière première pour toute la chaine d'activité

Préoccupation quotidienne des Français, la santé passe depuis quelques années à l'ère du numérique. L'e-santé regroupe plusieurs disciplines : la robotique, la télésanté

(réseaux sociaux, serious games...), la télémédecine (télésurveillance, maintien à domicile...) et la m-santé (tous les services liés à la santé disponibles sur un smartphone ou une tablette - m pour mobile -, comme les applis des objets connectés ou des capteurs sur le sommeil, le rythme cardiaque...). Le potentiel de croissance de la santé connectée est estimé à 4 à 7% par an d'ici 2020[1]. Les données recueillies via ces nouvelles technologies représentent une matière première indispensable pour toute la chaine d'activité du métier d'assureur. Car, l'enjeu est de mieux connaitre le client pour lui apporter des services et des produits personnalisés.

[1] Etude par Precepta intitulée L'e-santé au chevet du système de santé français (e-health at the bedside of the French health system) (2014).

Autant de données utiles également à d'autres services d'une compagnie d'assurance, comme le marketing pour créer des profils de clientèle et personnaliser leurs offres, proposer des renouvellements de contrats, faire des analyses statistiques et de recherches sur les sinistres, la prévention des délits, l'autorisation de crédits et autres vérifications permettant de tenir les dossiers clients à jour. Sans oublier que les assureurs peuvent être amenés à divulguer les données personnelles de leurs clients à des sous-traitants ou des fournisseurs de services comme des consultants, des conseillers spécialisés, des filiales du même groupe, des analystes de marché... au sein ou en dehors de l'Union européenne.

Les assurés redeviennent pleinement propriétaires de leurs données

Le RGPD clarifie les rôles et responsabilités de chacun pour que les clients puissent redevenir pleinement propriétaires de leurs propres données.

Il cherche également à redonner à chaque personne le droit de disposer de ses données et d'en contrôler les usages. Du côté des assureurs, le responsable de traitement doit veiller à ce que ces nouveaux droits soient effectifs via des outils comme des tableaux de bord, des formulaires en ligne facilement accessibles lorsque l'assuré souhaite faire part de son droit d'opposition et de rectification ou de son droit à l'oubli. Le RGPD exige également des entreprises qu'elles informent les personnes sur les différents traitements de données les concernant ; cette information doit être complète et porte notamment sur la finalité des traitements et la durée de conservation des données. Chaque document contractuel doit donc être modifié en ce sens, via une case à cocher par exemple.

Les contraintes posées par le RGPD apportent de nouvelles garanties de transparence pour l'assuré. De quoi, pour l'assureur, renforcer la confiance client et atténuer les craintes quant à l'utilisation des données personnelles. À titre d'exemple, lorsque l'assuré est susceptible de faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (tel un service d'assurance proposé ou non selon le profil de l'assuré), et qu'il y a consenti explicitement, il doit au moins pouvoir exprimer son point de vue, contester la décision automatisée le concernant, et solliciter une intervention humaine auprès de la compagnie d'assurance.

L'avis de l'expert

« En tant qu'unique entité dédiée à l'assurance, RCI Malta doit gérer des problématiques spécifiques à ce secteur, avec notamment un projet pour identifier les besoins et les impacts sur les métiers. Des workshops permettent de catégoriser les données personnelles. Les travaux de mise en conformité ont démarré au niveau de notre groupe depuis mars 2017. Des ateliers de suivi, avec une documentation approfondie sur la mise en œuvre et l'évangélisation du sujet, sont organisés chaque mois avec les différentes entités de RCI Corporate. »

Umberto D'AMICO,
IT Manager chez RCI Malta

40 ans de protection des données dans l'assurance

Loi n°78-17 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 modifiée par la loi du 6 août 2004 puis la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, définit les principes à respecter lors de la collecte, du traitement et de la conservation des données personnelles. Elle renforce les droits des personnes sur leurs données, prévoit une simplification des formalités administratives déclaratives et précise les pouvoirs de contrôle et de sanction de la CNIL. Cette loi sera modifiée d'ici au 25 mai 2018, afin de prendre en compte les changements résultant du RGPD, dont le principe d'accountability qui entraine la suppression de nombreuses déclarations CNIL auparavant obligatoires.

6 janvier

1978

1981

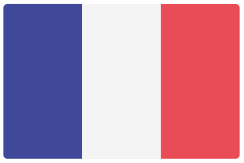
28 janvier

Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. C'est le premier instrument international contraignant qui a pour objet de protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel et qui réglemente les flux transfrontaliers des données.

Directive européenne n°95/46/CE sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Elle forme le cadre juridique général de la protection des données personnelles, détermine les grands principes d'un traitement loyal licite et adéquat, et liste les droits des personnes physiques (droit d'accès et de rectification), etc. L'article 28 exige de chaque État membre d'instituer une autorité de protection des données personnelles, sur le modèle général de la CNIL établie en France. Chaque État membre de l'UE a dû adopter une loi nationale pour transposer la directive dans leur droit interne, ce qui a entrainé certaines disparités entre les différentes lois nationales.

24 octobre

1995



2014

Novembre

Pack de conformité Assurance signé entre la CNIL et l'ensemble des assureurs pour marquer leur volonté de déployer les technologies numériques et d'exploiter les données personnelles avec responsabilité et exemplarité. Objectifs : une régulation efficace qui protège les personnes physiques et une exploitation efficace des données recueillies pour les entreprises du secteur.

2017

Octobre

Pack de conformité Assurance Véhicules connectés. L'enjeu est d'intégrer la dimension « protection des données personnelles » dès la phase de conception des produits (c'est la notion de Privacy by Design du RGPD) et d'assurer la transparence et le contrôle par les personnes de leurs données.

2016

27 avril

Adoption du Règlement n°2016/679 par le Parlement Européen et le Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. C'est le RGPD qui vient abroger la Directive Européenne n° 95/46/CE, et instaurer un socle d'harmonisation minimum au sein de l'UE.

2018

25 mai

Entrée en application du RGPD. À compter de cette date, les entreprises devront être en conformité avec les dispositions du RGPD. La mise en conformité est une démarche globale et continue, qui s'inscrit dans la durée.

PARTIE 2

APPLICATION MÉTIER DU RGPD AU MONDE DE L'ASSURANCE

Une exploitation des données personnelles contrôlées, plus de confiance client

Comment le RGPD transforme les métiers de l'assurance

Le volume des données a augmenté de manière exponentielle ces dernières années. L'Assurance est un des secteurs ayant intérêt à les exploiter et les valoriser afin de proposer à ses clients les offres les plus adaptées. Avec l'entrée en application du RGPD et de nouvelles règles de protection des données, quelles conséquences concrètes pour le métier et comment saisir cette opportunité pour transformer sa façon de gérer les données et faire évoluer sa relation client?

Plus de la moitié des acteurs de l'assurance (et de la banque) ont d'ores et déjà identifié et initié des chantiers concernant le RGPD, selon une enquête Optimind Winter réalisée en été 2017. Rien d'étonnant quand on sait que la réglementation sectorielle sur les données à caractère personnel est déjà bien prégnante depuis plusieurs années (voir notre timeline 40 ans de protection des données personnelles page 9). Si le RGPD est clairement identifié par les assureurs et les mutualistes, reste encore plusieurs points d'achoppement, comme la conciliation avec la directive sur la distribution d'assurance (DDA), la cartographie des données, la sensibilisation des collaborateurs et la transformation de la relation client.

Comment concilier DDA et RGPD?

2018 sonne comme une année charnière avec non seulement l'entrée en application du RGPD le 25 mai, mais également la directive sur la distribution d'assurance (DDA), trois mois plus tôt.

La DDA, qui succède à la directive sur l'intermédiation en assurance (DIA1), vise à renforcer la protection des consommateurs dans leurs relations avec tous les distributeurs d'assurance. Problème : les principes institués par le RGPD et la DDA peuvent parfois venir en contradiction. Par exemple, le RGPD impose de ne recueillir que les données nécessaires à l'accomplissement du traitement, alors qu'avec la DDA un assureur se doit de collecter les informations liées aux besoins et aux exigences du client pour lui proposer un produit adapté. Dans le cas d'un produit d'assurance-vie, une compagnie, au vu de la DDA, peut tout à fait se renseigner sur le profil de risque du client même si ces informations ne sont pas directement liées à la distribution du produit. Dans le cadre du RGPD, cela ne pourra se faire que s'il est possible de prouver que cela est nécessaire au regard des finalités du traitement, de la bonne exécution du contrat, ou du respect des obligations légales incombant à la compagnie d'assurance.

"Pour un produit d'assurance-vie, une compagnie, au vu de la DDA, peut tout à fait se renseigner sur le profil de risque du client, même si ces informations ne sont pas directement liées à la distribution du produit. Dans le cadre du RGPD, cela est impossible du fait de l'obligation d'utiliser uniquement les données nécessaires au traitement."

La DDA demande également que les responsables de traitements (ainsi que leurs sous-traitants) tiennent des registres où figurent un certain nombre de données liées à la relation client. Or, le RGPD impose des règles strictes en matière de conservation des données et de délai de conservation. Quelle serait donc la durée de conservation la plus pertinente pour disposer d'une maitrise suffisante de son dispositif de distribution tout en respectant le droit des personnes physiques ? « On peut répondre à une loi et être en contradiction avec une autre », remarque Philippe Bouvier, Product Manager chez Wyde. « Pour établir un contrat de prévoyance, le prospect répond à un questionnaire médical pour savoir s'il est considéré comme une personne à risques. L'assureur doit garantir qu'il utilise ces données au moment de la tarification avant de les supprimer si elles ne répondent pas à une obligation réglementaire de conservation ou d'utilisation dans un traitement. Il est donc important de mettre en place un système de suppressions ou d'anonymisation des données.

Notre Conseil

La DDA ne couvre pas les champs d'application relatifs à la protection des données personnelles. Répondre à **la mise en conformité du RGPD est une priorité,** aussi bien stratégique pour rester dans la course, que financière au vu des lourdes sanctions possibles.

Quelles sont les nouvelles relations à établir avec les sous-traitants?

Le sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et de responsabilité. Il fait dorénavant figure de conseil auprès du responsable de traitement pour la conformité à certaines obligations du RGPD (failles de sécurité, destruction de données, contribution aux audits...). « Mon cheval de bataille en tant que DPO est la chaine de sous-traitance, car il est important de comprendre que si un seul maillon n'est pas conforme ou ne met pas en place des mesures de sécurité, c'est toute la chaine qui est affaiblie », insiste Adèle Adam DPO de Claranet, société spécialiste de l'infogérance d'applications critiques. Car le RGPD étend les responsabilités des sous-traitants. En tant qu'hébergeur de données sur certaines offres de services liées notamment à la santé et à la banque, Claranet travaille sur le renforcement des contrats, comme le prévoit l'article 28 du RGPD. « Il manquait certaines thématiques dans les contrats de services type de Claranet, comme les clauses de sous-traitance ultérieures. Il a fallu réviser nos modèles pour proposer à nos clients une trame conforme aux exigences du RGPD."

Notre Conseil

La transparence et la sécurité des données personnelles dépassent les frontières de l'organisation. Les sous-traitants sont également directement concernés. En tant que garant des données de vos assurés, il est de votre responsabilité de **faire appel à des partenaires présentant toutes les garanties en matière de protection des données**. Un seul maillon faible de cette chaine de conformité pourrait anéantir tous vos efforts de bonne réputation en la matière. Le sous-traitant peut être contrôlé et sanctionné par la CNIL au même titre que le responsable de traitement. Chaque maillon doit être en capacité de démontrer sa conformité et garantir que les prestataires, aussi bien en amont qu'en aval de la chaine de sous-traitance répondent aux exigences.

Comment sensibiliser tous les collaborateurs à la protection des données personnelles?

Les grands acteurs de l'assurance disposent d'ores et déjà d'équipes mobilisées sur le RGPD, dont certaines portent la bonne parole dans les filiales et les branches », explique Quang Nghiem, conseiller chez Crysal, cabinet partenaire de Wyde spécialisé en Assurance santé et Protection sociale. Quant aux mutuelles indépendantes, elles n'ont pas encore atteint un haut niveau de maturité sur le sujet. La sensibilisation des enjeux liés à cette nouvelle problématique passe par la formation des collaborateurs. Ainsi toute personne qui intervient sur un projet doit être sensibilisée aux règles de sécurité des données personnelles, aux risques liés à ces données ainsi qu'aux droits des personnes physiques en la matière. Le Data Protection Officer peut réaliser en interne cette sensibilisation, tout comme des organismes agréés : « Nous renforçons nos actions de sensibilisation via une plateforme de e-learning comportant des parcours dédiés à la sécurité et à la protection des données personnelles. La notion de "donnée personnelle" au sens de la loi reste abstraite pour de nombreuses personnes. Une adresse e-mail professionnelle est une donnée personnelle par exemple, car elle permet d'identifier une personne physique », insiste **Adèle Adam.**

"La notion de "donnée personnelle" au sens de la loi reste abstraite pour de nombreuses personnes. Une adresse e-mail professionnelle est une donnée personnelle par exemple, car elle permet d'identifier une personne physique"

Outre le front-office, tous les métiers de l'entreprise sont concernés par le RGPD : le marketing qui valorise les données, mais aussi les techniciens (développeur, intégrateur...) ou encore les collaborateurs en lien avec les sous-traitants. Car, le RGPD implique une revue des contrats avec les clients et les fournisseurs. Il rend obligatoire la conclusion de certains accords avec les sous-traitants ou de clauses contractuelles fixant l'étendue des responsabilités. Il est important de revoir les politiques de sous-traitance en y intégrant la notion de co-responsabilité qui permet de se prémunir des conséquences liées aux fuites de données lors d'activités externalisées.

Notre Conseil

Parce que les règles concernant les données personnelles doivent devenir un automatisme pour tous vos collaborateurs, sensibilisez-les à ce nouvel enjeu. **Multipliez les supports numériques de formation et de documentation** pour attiser leur curiosité et renforcer leur prise de conscience.

Quels sont les impacts sur la gestion et la relation client?

Parmi les six fondements possibles permettant d'avoir un traitement licite, il y a le consentement explicite : « La logique du consentement explicite pour chaque traitement de données transforme la façon d'appréhender la relation client. Dorénavant, il faut exercer son métier d'agent général avec les données personnelles strictement nécessaires. S'il a besoin de plus d'informations, il faut demander le consentement du client et expliquer la finalité de l'utilisation de la donnée », prévient Quang Nghiem. Dans ces circonstances, comment continuer d'exploiter les données ? Car il est devenu indiscutable que cette exploitation et valorisation des données permettent d'améliorer les prédictions et d'avoir un temps d'avance sur ses concurrents en matière de services et produits personnalisés.

"La nouvelle logique du consentement explicite pour chaque traitement de données transforme la façon d'appréhender la relation client".

Le défi de la relation et de la confiance client est un réel enjeu business pour les prochaines années dans le secteur assurance. « Les assureurs veulent de plus en plus capter de données : le RGPD permet de "tout" faire pourvu qu'on le fasse dans le respect des règles établies. Si on veut conserver un maximum de données, il suffit de les anonymiser pour ne plus remonter à leur propriétaire et de les archiver au fur et à mesure que les délais de conservation sont dépassés. C'est très nouveau, et cela transforme le commerce, la gestion et la relation client », insiste **Quang Nghiem**.

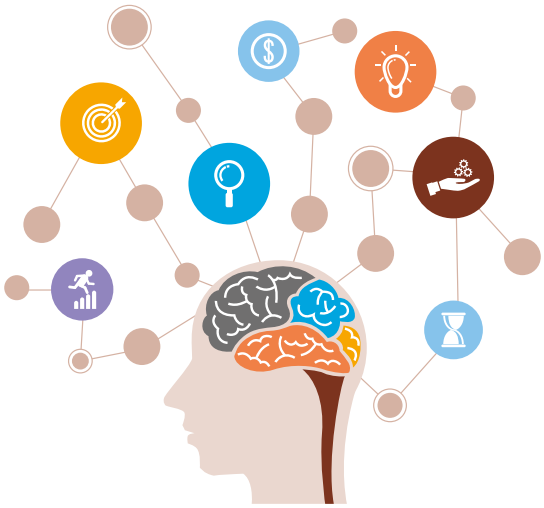
Pour les gestionnaires d'assurances (qui utilisent les applications, collectent et exploitent les données), le RGPD renforce plusieurs paramètres, comme l'obligation de communiquer aux clients et prospects, avant la signature d'un contrat, l'ensemble des données collectées et leur usage au-delà de la gestion du contrat. Ils ont donc pour tache de recueillir leur consentement formel et explicite. « L'article 6 du RGPD définit les six différents fondements permettant d'avoir un traitement licite, et parmi eux, il y a le traitement nécessaire à l'exécution d'un contrat avec la personne, ou encore, le consentement de la personne pour une ou plusieurs finalités spécifiques. Ce consentement libre et éclairé doit pouvoir être démontré. Il s'agira de cases à cocher par exemple avec des informations complètes sur le traitement dans le contrat d'assurance », précise **Maître Clara Petit**, avocate spécialiste en données personnelles et e-réputation, **Cabinet Itenau Avocats.**

Notre Conseil

Ne considérez pas le RGPD comme une série de contraintes ou un frein à l'exploitation des données. Voyez plutôt **l'opportunité de renforcer la confiance avec vos assurés.** Être en conformité avec le règlement est un facteur différenciant à terme pour se démarquer de la concurrence et afficher ses bonnes pratiques en matière de protection des données personnelles. Nous pouvons imaginer des organismes certifiant le niveau de mise en conformité : ce serait alors un élément marketing fort.

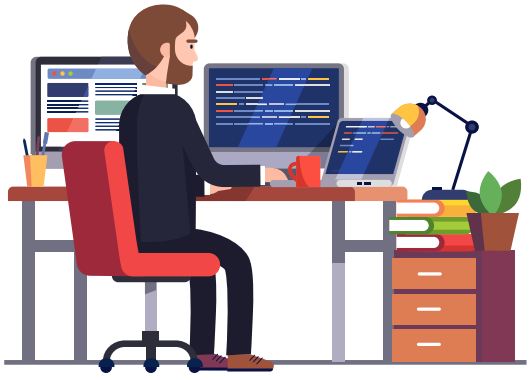
Meilleures pratiques « assurance » pour passer au RGPD

Le 25 mai 2018 est une date butoir pour mettre en œuvre les premières actions de mise en conformité. La CNIL est particulièrement attentive aux preuves de conformité et aux efforts des entreprises. Best practices pour s'y préparer.



Pensez transversalité

Conserver par exemple les données d'un prospect pendant trois ans, comme le prévoit la norme simplifiée n°48 de la CNIL, est un principe valable pour le front-office qui a besoin d'informations relativement récentes. Au terme de ce délai, le responsable de traitement reprend contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite, les données devront être supprimées ou archivées conformément aux dispositions en vigueur. Les décisionnaires, les actuaires ou encore le marketing peuvent eux avoir besoin de deux ans supplémentaires pour établir des analyses statistiques fiables et avoir une meilleure connaissance des risques (nombre de sinistres...). Il est donc important de gérer les politiques d'accès aux données et de durée de conservation des données en fonction des différentes finalités pour lesquelles elles sont traitées, et pour satisfaire tous les usages métiers.



Travaillez main dans la main avec votre éditeur de logiciels

Apprenez à restreindre les accès utilisateurs. Par exemple, le service de prestations de santé sera le seul à avoir accès à certaines données sensibles, car le service cotisations n'a pas besoin d'accéder à ces informations. Plus un grand nombre d'individus a accès à des données dont ils n'ont pas besoin pour accomplir leurs tâches, plus les risques en termes de sécurité sont avérés. Afin de cibler les gestionnaires dédiés, il faut cartographier l'ensemble des données : cela peut faire l'objet d'un travail collaboratif entre l'éditeur de logiciels et l'organisme de l'assurance. Dans les petites structures, où les collaborateurs sont polyvalents, c'est une véritable conduite du changement qu'il faut mettre en place, à la fois culturel, organisationnel et technique.

Nommez un DPO au profil hybride

Le Data Protection Officer (DPO) est le véritable chef d'orchestre de la conformité. Sa désignation est rendue obligatoire dans les entreprises faisant des traitements à grande échelle de suivi régulier et systématique des personnes ou de données sensibles. « Lorsqu'un DPO est requis, nous préconisons la désignation d'un DPO interne. D'un point de vue opérationnel, il devra comprendre l'architecture de son entreprise, et les considérations juridiques et pratiques découlant du secteur d'activité concerné. Il devra être facilement joignable par les collaborateurs », conseille **Maître Clara Petit**.

Le DPO peut être hybride : un juriste qui comprend le langage informatique ou un informaticien qui connait les contraintes juridiques. Si en plus de cela, votre DPO possède déjà une expertise métier dans l'assurance ou est un ancien CIL (Correspondant Informatique et Libertés) ayant évolué dans le secteur, alors l'ensemble de l'expertise requise sera couverte. Car, entre autres missions, il est chargé de s'assurer que son entreprise respecte la réglementation en matière de protection des données personnelles ; d'assister les responsables des traitements et les collaborateurs impliqués en les informant, en les conseillant mais également en contrôlant la mise en œuvre de leurs fichiers ; de coopérer avec la CNIL ; de mener des études d'impact pour les traitements à risques élevés, et enfin de garantir par défaut le plus haut niveau de sécurité des données.

L'avis de l'expert

« La nomination d'un DPO devient obligatoire dans les entreprises qui effectuent des traitements à grande échelle de suivi régulier et systématique des personnes ou de données sensibles. En tant qu'infogérant d'applications critiques, Claranet entre complètement dans cette configuration. Il est important pour nous de rassurer nos clients en leur montrant que nous prenions le sujet à bras le corps. Jusque-là, le Correspondant Informatique et Libertés (CIL) s'occupait uniquement du traitement interne des données. Avec l'arrivée du Data Protection Officer (DPO), il faut avoir la capacité à adresser notre conformité interne (rôle de Responsable de Traitement) et nos prestations de service (rôle de Sous-Traitant). »

Adèle Adam

DPO et chargée de conformité sur l'offre e-santé de Claranet

PARTIE 3

PRISE EN COMPTE DES CHANGEMENTS RÉGLEMENTAIRES AU NIVEAU DES OUTILS DE GESTION

Check-list à l'intention des DSI

Distiller l'état d'esprit RGPD jusque dans les outils

En matière de SI, il ne s'agit pas simplement de rajouter une strate de sécurité pour être en conformité avec le RGPD mais de transformer l'ensemble du système. Les informaticiens doivent désormais s'intéresser de très près aux données, leur nature et leur cycle de vie, car il va falloir être capable de dire où sont stockées ces données, lesquelles sont considérées comme personnelles... Pour cela, il est indispensable d'établir une check-list des priorités.

Les consommateurs accordent majoritairement leur confiance aux banques et aux assurances (83%), en matière de cybersécurité et de protection des données. Le secteur de l'e-commerce recueille à peine 30%, les télécoms et la grande distribution seulement 13%. Paradoxe : seulement un responsable sur cinq du secteur banque et assurance considère être en mesure de détecter et contrer les cyberattaques . Face à cette confiance, les assureurs n'ont plus qu'à profiter de l'opportunité RGPD pour se montrer à la hauteur des attentes de leurs clients. Car, on estime à 30 milliards d'euros le coût du vol de données en France. 90% des vulnérabilités sont concentrées dans les applications alors que 80% des budgets sécurité sont consacrés à l'infrastructure . Conclusion : il est nécessaire de revoir la politique de sécurisation pour prévenir les risque de cyberattaques.

Comment sécuriser des milliers de données stockées dans le SI?

La garantie de la sécurité des données personnelles est un point important du RGDP. Au-delà des mesures préventives à prendre pour protéger les données, il faut informer sous 72 heures la CNIL en cas de compromission, d'altération, de divulgation ou d'accès non autorisé, ou de perte de données. « Claranet a adapté ses processus (certifiés ISO27001 depuis 2011), notamment en matière de notification des violations de la sécurité des données. Pour que notre client puisse être en capacité d'évaluer les impacts et de remonter si. nécessaire les violations aux autorités et aux personnes concernées, la nature de l'incident, un des critères obligatoires du RGPD, a été ajouté à l'outil de ticketing », explique **Adèle Adam.**

"90% des vulnérabilités sont concentrées dans les applications alors que 80% des budgets sécurité sont consacrés à l'infrastructure."

Renforcer les systèmes de protection passe nécessairement par la multiplication des tests d'intrusion et des audits. L'intelligence artificielle pourra aider à analyser les logs et rechercher d'éventuelles fraudes.

Notre Conseil

En matière de cybersécurité, il n'y a aucune place à l'attentisme : il est indispensable de **multiplier les tests d'intrusion,** de les mettre régulièrement à jour et de lancer des audits annuels. L'anonymisation donnera par exemple l'assurance de minimiser les dégâts en cas d'accès non autorisé ou de violation de données, étant rappelé que les données réellement anonymisées ne sont plus considérées comme des données personnelles.

[2] Rapport publié par le Digital Transformation Institute de Capgemini intitulé « The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure (2017).

[3] Étude EMC menée en 2014.

Comment cartographier les données?

Dans le cadre du futur règlement européen, les entreprises ont l'obligation de tenir un registre des activités des traitements des données. Pour recenser précisément toutes ces données, une cartographie s'impose. Des milliers de données sont répertoriées, quelle que soit la branche métier (santé, épargne, prévoyance...), le plus compliqué est de les identifier. Pour cela, il faut avoir une bonne connaissance de l'architecture des outils. Une fois l'identification au niveau des métiers établie, c'est aux architectes techniques d'identifier au cas par cas les différentes données. « Il est recommandé d'installer un processus automatisé mais l'impératif humain demeure. Il s'agit d'identifier le collaborateur avec la meilleure connaissance de l'outil », selon Philippe Bouvier. Aux architectes techniques également d'aller chercher les données cachées. Pour cela, il mènera une évaluation de la base de données de l'outil. Pour savoir où chercher, il faudra un profil connaisseur de la modélisation des outils.

"Les données personnelles sont dispersées dans l'ensemble de l'architecture SI de l'organisation. Les recenser intégralement est un travail qui s'inscrit dans la durée."

La première tâche consiste à établir la cartographie de traitement pour voir où sont les données. « Pour cela, il est nécessaire de rencontrer toutes les équipes internes pour comprendre comment elles travaillent. Nous avons mené plusieurs entretiens mais la cartographie est mouvante : elle évolue à chaque nouvelle collecte de données, d'où l'importance de la transversalité entre les métiers", explique **Adèle Adam**.

Ainsi, cartographier les traitements de données personnelles permet de recenser les catégories de données (bancaires, santé, biométriques, numéro de sécurité sociale...), les finalités pour lesquelles elles sont recueillies, les acteurs (internes ou externes) qui les traitent, ainsi que les flux et les éventuels transferts hors de l'Union européenne. « Nous avons lancé un projet de data management pour identifier les données, puis lancé un process d'anonymisation et de développement customisé. Il ne s'agit pas simplement de problématiques réglementaires mais de mise en oeuvre de chantiers complexes », constate Umberto d'Amico. Toutes ces données doivent être rapidement accessibles pour permettre aux particuliers de les modifier, les supprimer (droit à l'oubli) ou les faire transférer (droit à la portabilité). Les données clients sont présentes dans les logiciels métiers mais aussi dans différents documents des équipes marketing, dans les rapports de la direction, voire dans les mails des courtiers. Bref, toutes ces informations sont dispersées un peu partout dans l'architecture SI, sans oublier tous les dossiers papiers rangés dans les armoires des petites structures. Les recenser entièrement se révèle être un travail de longue haleine.

Notre Conseil

Recenser toutes les données personnelles est un travail long et fastidieux mais une étape importante vers la mise en conformité. Pour une vision globale et exhaustive, tous les métiers sont mis à contribution. Dans votre cartographie de traitement, pensez à bien faire apparaitre toutes les personnes responsables (soit du traitement soit des services opérationnels), ainsi que les sous-traitants ayant accès à ces données ; identifier les catégories de données et celles considérées comme les plus à risques ; indiquer la finalité pour laquelle vous collectez ces données et la durée de conservation.

"Toutes les données doivent être rapidement accessibles pour permettre aux particuliers de les modifier, les supprimer ou les faire transférer."

Comment mettre en œuvre le droit à l'oubli?

Le RGPD permet d'exercer son droit à l'oubli, c'est-à-dire le droit de voir ses données personnelles effacées, dans six cas de figure précis:

- les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées
- le consentement était nécessaire lors de la collecte des données (ce qui vise en particulier les cas des données sensibles), et la personne concernée a retiré son consentement ;
- soit la personne exerce son droit d'opposition « pour des raisons tenant à sa situation particulière » lorsque le traitement est basé sur une mission d'intérêt public ou sur un intérêt légitime. Le responsable de traitement doit alors démontrer l'existence de motifs légitimes et impérieux pour s'y opposer. Soit la personne s'oppose à ce que ses données soient traitées à des fins de prospection, dont le profilage
- les données ont fait l'objet d'un traitement illicite ;
- les données concernent un mineur
- l'effacement est prévu par une obligation légale (nouvelle loi ou décision de justice par exemple)

L'effacement des données englobe également l'effacement de tout lien vers les données, ou toute copie ou reproduction des données.

Ces restrictions sont un levier de souplesse pour mettre en place le droit à l'oubli. D'ailleurs, le règlement prévoit de tenir compte des technologies disponibles et des coûts de mise en œuvre.

NOTRE CONSEIL

Avant qu'une personne ne puisse exercer son droit à l'oubli, nous vous conseillons de **prévoir différents types d'archivage,** un premier sur une base active, un second intermédiaire pour les services juridique ou du contentieux, et une dernière étape où les données seront supprimées ou anonymisées. Il est également possible de prévoir des cas où certaines données sont conservées, puis elles sont transformées en statistiques pour avoir un recul sur la gestion client. L'idée est de toujours traiter le minimum de données utiles au traitement.

L'avis de l'expert

"Beaucoup d'organisations travaillent sur le recensement de leurs données : où sont-elles stockées ? Dans des dossiers papier ? Dans des archives type base de données ? Chez les sous-traitants ? Une fois les catégories de données identifiées, il est indispensable de s'interroger sur la politique de consentement à appliquer. Une phase de cadrage va permettre d'évaluer le niveau de conformité de l'existant par rapport au nouveau règlement, sur un plan juridique, organisationnel et informatique. Si cette première road map générale ne suffit pas à se mettre en conformité, elle a le mérite de montrer à la Cnil que l'entreprise a mis en œuvre une première preuve indispensable pour limiter les risques de sanction !"

Quang Nghiem
Conseiller Chez Crysal

Notre solution

Wynsure en conformité avec la portabilité des données inscrite dans le RGPD

La suite de solutions Wynsure supporte les fonctions commerciales et les meilleures pratiques du secteur de l'assurance à travers la gestion du cycle de vie de bout en bout de l'ensemble de l'écosystème. Un outil d'ores et déjà ancré dans de bonnes pratiques en matière de protection de données, et qui se renforce avec l'arrivée de nouveaux principes comme la portabilité des données et le droit à l'oubli.

"Notre rôle en tant qu'éditeur de logiciels est aussi de sensibiliser nos clients aux impacts du RGPD sur le métier d'assureur et de montrer que nous aussi nous y travaillons », assure Philippe Bouvier, Product Manager chez Wyde. Wynsure est une suite de solutions qui combine un front-office moderne basé sur un puissant back-office (haute configurabilité, ensemble des modules de l'assurance…) dans une plateforme unique pour la distribution homogène à travers tous les canaux numériques.

Du reporting pour extraire toutes les données

"Nous conseillons de mettre en place les modifications permettant de proposer le plus rapidement possible un produit conforme au RGPD, et notamment la notion de portabilité des données », ajoute Philippe Bouvier. Les équipes de Wyde suggèrent donc sur la mise en place d'une solution de reporting permettant d'extraire n'importe quelles données. « À terme, l'objectif est d'avoir tout le périmètre de l'outil accessible."

Un portail client pour le droit à l'oubli

Wyde pousse à travailler sur la mise en place d'un portail pour le droit à l'oubli. Ce portail client semble un outil indispensable et pratique pour conserver la maitrise des données et avoir en temps réel les modifications apportées par le client, que ce soit un changement de coordonnées, une suppression d'informations ou encore une demande de consentement. « Dans les dix ans à venir, tout dossier papier devrait disparaitre car ce format va à l'encontre des exigences du RGPD que sont le suivi et la maitrise des données. Avec le papier, il est impossible de savoir quel collaborateur, interne ou externe, a pu accéder aux informations client. Le portail web est le canal de communication idéal entre un assureur et son client », conclut **Philippe Bouvier**.

Meilleures pratiques pour bien s'outiller

Security by design, portabilité des données, protection des données dès la conception... Autant de nouveaux concepts à maitriser. Best practices pour s'y préparer.

Pensez Security by design

L'approche dite Security by design englobe les modélisations des risques et des menaces dès la phase de conception d'un outil ou d'une solution. Cela passe par l'évaluation des principaux points de vulnérabilité, l'analyse des risques auxquels l'entreprise est particulièrement sensible, l'analyse des outils de supervision et leur capacité à détecter, qualifier et notifier une violation, et enfin par la sensibilisation des équipes de conception d'application. Une entreprise doit pouvoir savoir qui de ses collaborateurs, de ses clients, de ses fournisseurs créent de la donnée dans son SI, accède à ces données et aux applications. C'est ici l'opportunité de renforcer les différents systèmes d'authentification.

Utilisez le reporting pour exporter les données

La tendance est de trouver une solution globale pour la portabilité des données. Le reporting est un outil natif pour certains grands groupes d'assurance. Pour d'autres, de plus petites organisations, il faudra mettre en place des traitements spécifiques pour extraire les données, comme la gestion manuelle d'identification de la personne, la demande d'extraction de données... Limite : l'assureur n'aura pas l'entière maitrise de ces processus. Il aura besoin de faire appel à l'éditeur de l'outil. Il sera également important d'auditer l'outil pour voir s'il répond au RGPD.

Appliquez la protection des données personnelles dès la conception et par défaut

Les concepts de « privacy by design » et de « privacy by default » supposent de penser la protection des données personnelles en amont de la conception d'un produit ou d'un service. Cela signifie mettre en place un minimum de mesures techniques organisationnelles et juridiques, comme la pseudonymisation ou l'anonymisation des données. Un gestionnaire de bases de données (DBA) peut se charger de cette tâche avec un générateur automatique de chiffrement de données. Cette implémentation implique tous les métiers participant au processus (marketing, juridique, gestionnaire, statistiques...).

Auditez vos outils régulièrement

Un audit à minima annuel est conseillé pour s'assurer des mises à jour. L'éditeur de logiciel devra créer des points de contrôle, tout cela sans perturber les phases de développement. « Ce sera aussi un élément déterminant pour nous éditeur : à chaque sortie de version, nous ferons un audit pour nous assurer de la mise en conformité. Nous sommes les garants de cette brique qui sera intégrée dans le SI des groupes d'assurance ", stresses **Philippe Bouvier**.

A PROPOS DE L'AUTEUR

PHILIPPE PAYET

DIRECTEUR GÉNÉRAL EUROPE, WYDE

Philippe gère les Opérations de Mphasis Wyde Europe. Il est responsable de la Stratégie Go to Market, du développement commercial et supervise les Opérations de déploiement des Solutions Technologiques. Avec à son actif plus de 18 ans dans le secteur des nouvelles technologies en assurance et télécommunications, Philippe dispose d'une connaissance approfondie du secteur de l'assurance et a géré avec succès de grands comptes Européens de l'industrie des Telecom et de l'Assurance.