



RGPD : Malakoff Médéric déploie cinq chantiers

Alors que la date butoir du 25 mai 2018 approche, Malakoff Médéric se prépare à la conformité au texte européen. Le projet, initié en février 2017 et qui repose sur cinq grands chantiers, entre dans sa phase de déploiement.

Le règlement général sur la protection des données personnelles (RGPD) entrera en application le 25 mai 2018 au niveau européen. S'il concerne tous les secteurs, ce texte a une implication particulière pour certains domaines comme celui de l'assurance santé et des mutuelles, qui traitent des données de santé de leurs adhérents. Le groupe de protection sociale Malakoff Médéric intervient pour l'assurance santé et prévoyance de 6,6 millions d'assurés à titre collectif et/ou individuel, et gère la retraite complémentaire de 2,8 millions de salariés et 2,9 millions de retraités allocataires. La RGPD concerne ainsi les données personnelles des assurés (âge, sexe, s'ils ont des enfants, nom de leur employeur...) ainsi que leurs données de santé.

Un projet RGPD initié en février 2017

Pour nous mettre en conformité avec le règlement européen, "en février 2017, nous avons lancé le projet RGPD. La phase de cadrage du projet a été terminée en juin", confie [Johanna Carvais-Palut](#), responsable protection des données à caractère personnel et Correspondante informatique et libertés (CIL) de Malakoff Médéric. Si l'objectif de ce projet est de répondre au règlement européen, tous les chantiers ne seront probablement pas totalement terminés en mai 2018. "Nous serons conformes sur beaucoup de choses et nous aurons une bonne feuille de route pour le reste. Il s'agit d'un changement de culture. Le projet ne s'arrête pas en mai 2018. La protection des données va vivre grâce à cette gouvernance que nous mettons en place", indique la responsable du projet. Le groupe se trouve ainsi en ligne avec les résultats de l'étude [d'Optimind Winter](#) réalisée en juillet 2017 auprès d'acteurs du [monde de l'assurance, de la banque et de la santé](#). Sur la centaine de répondants, 54 % avaient identifié et démarré les principaux chantiers tandis que 24 % prévoient de lancer les chantiers en janvier 2018 et 22 % n'étaient pas au courant.

Ce projet repose sur cinq principaux chantiers: la gouvernance, le droit des personnes, les relations avec les tiers, l'accountability ou "l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données", selon la CNIL et la notification des violations de

données. Si la responsable de la mise en œuvre de l'ensemble du projet ne cite pas le montant du budget consacré à la mise en conformité, elle précise que celui-ci est conséquent. En termes de ressources humaines, Johanna Carvais-Palut s'appuie actuellement sur un chef de projet à plein temps et sur une filière de relais DPO (délégué à la protection des données) en cours de mise en place.

Chantier 1 : La gouvernance

En matière de gouvernance, la première étape a été d'identifier le futur DPO, "chef d'orchestre de la conformité", selon la CNIL qui [détaille cette fonction](#). Johanna Carvais-Palut désignée CIL en mars 2017 prendra cette fonction officiellement en janvier 2018. Elle s'appuiera sur une filière de "relais DPO", qui sera officialisée en décembre 2017 et constituée d'une vingtaine de collaborateurs, présents au sein de différentes entités métiers, services support... "Ils ont suivi une formation labellisée par la CNIL. L'objectif est de faire monter en compétence les relais DPO et de diffuser la culture au sein des différentes directions", détaille Johanna Carvais-Palut. Les premières réunions devraient concerner la mise en place d'actions en interne et en externe pour promouvoir la journée internationale de protection des données du 28 janvier 2018. L'objectif est de sensibiliser les 5 600 collaborateurs du groupe à la question. La responsable mène actuellement des actions de formation auprès des différents comités de direction. Pour toucher le plus grand nombre, Malakoff Médéric utilisera un serious game. "Nous voulons proposer la formation sous un angle ludique pour laisser les collaborateurs libres de suivre le parcours de formation à leur façon. Nous sommes en train de choisir le prestataire pour un lancement prévu en mai 2018", indique Johanna Carvais-Palut, sans préciser l'investissement prévu.

Chantier 2 : Le droit des personnes

Le deuxième chantier concerne le droit des personnes, c'est-à-dire "la transparence, l'information des personnes et la gestion des consentements", détaille Johanna Carvais-Palut. "Ce chantier est celui qui prendra le plus de temps", indique la responsable.

Le groupe change actuellement de ■■■

Malakoff Médéric

5 600 salariés

Assurance de personnes (santé, prévoyance, épargne retraite) :

3,8 milliards d'euros de chiffre d'affaires récurrents en 2016 et 212 000 entreprises assurées pour la santé et la prévoyance

Retraite complémentaire :

10,8 milliards d'euros de cotisations encaissées et 16,5 milliards de prestations versées en 2016.



Nous devons être en capacité de prouver notre conformité et faire du privacy by design une réalité. Il faut intégrer la protection des données dès la conception »

Johanna Carvais-Palut
Malakoff Médéric

■■■ système d'information, ce qui implique une modification de l'intranet pour permettre notamment le recueil des consentements et leur retrait. En parallèle, le groupe a recensé plus de 500 documents à mettre à jour, signale Johanna Carvais-Palut. Les travaux portent également sur les cookies, précise la responsable de la protection des données personnelles. *“L'objectif est que l'assuré soit maître de ses données et de l'accompagner au mieux dans tous les nouveaux services. À terme, nous voulons lui laisser la main pour gérer ses données et lui proposer des services adaptés à ses besoins”,* ajoute-t-elle.

Chantier 3 : Les relations avec les tiers

Dans le cadre du 3^e chantier, Malakoff Médéric a recensé ses principaux contrats partenaires, fournisseurs... pour les adapter au RGPD. Comme le précise la CNIL, le règlement européen entraîne une modification dans la responsabilité : *“Alors que le droit de la protection des données actuel concerne essentiellement les “responsables de traitements”, c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.”* Pour y répondre, Malakoff Médéric analyse l'impact du RGPD sur ses contrats et travaille avec ses prestataires sur *“l'ajout de clauses et d'avenants pour les contrats en cours”,* note Johanna Carvais-Palut.

Chantier 4 : L'accountability

“Le chantier le plus conséquent est celui qui concerne l'accountability (responsabilisation). Nous devons être en capacité de prouver notre conformité et faire du privacy by design une réalité. Il faut intégrer la protection des données dès la conception”, indique la responsable de la protection des données personnelles. Dans ce cadre, elle a créé un référentiel unique de durée de conservation des documents,

par exemple. De plus, Malakoff Médéric va acquérir deux outils dédiés à la conformité, pour lesquels la sélection des prestataires est en cours. *“Le premier concernera le pilotage et la gestion de la conformité des traitements”,* explique Johanna Carvais-Palut. Le second porte sur la saisie des documents liés aux contrats avec les assurés et notamment des zones de commentaires libres. *“Cet outil permettra le filtrage des zones de commentaires. Il permettra de s'assurer que dans les zones de commentaires, seules des données objectives sont ajoutées”,* détaille la responsable. Alors que des contrôles sont déjà effectués afin de s'assurer de la pertinence des commentaires ajoutés aux dossiers, elle prévoit notamment d'utiliser un filtrage automatique des commentaires extraits de ces zones avec une liste de mots interdits. Les zones de commentaires seront alors passées au crible d'outils de filtrage, ce qui permettra d'augmenter le nombre de contrôles.

Chantier 5 : La notification des violations de données

Avec la RGPD, les entreprises doivent notifier à l'autorité de contrôle dans les 72 heures une violation de données personnelles et dans certains cas aux personnes dont les données sont concernées. Sur ce point, Johanna Carvais-Palut se montre confiante : *“nous avons déjà une politique de gestion des incidents de sécurité. Nous allons ajouter la dimension privacy”.* En parallèle de ces différents chantiers, le groupe travaille également sur la communication de ces changements auprès des assurés. *“Nous avons commencé à aborder la question du RGPD dans le guide que nous envoyons aux assurés avec leur carte de tiers payant. Nous les informerons également lorsque l'espace intranet aura été modifié pour les nouveaux paramètres”,* détaille Johanna Carvais-Palut. À mi-parcours et après une période de définition, le projet RGPD de Malakoff Médéric passe dans sa phase de réalisation. ■

Aurélie Dureuil

mind Health, une nouvelle plateforme dédiée à l'e-santé

Cet entretien a été réalisé par la rédaction de *mind Health*, nouvelle plateforme d'information business intelligence dédiée au secteur de la santé. Éditée par Frontline Media et en cours de lancement, *mind Health* s'adresse aux laboratoires pharmaceutiques, sociétés de dispositifs médicaux, fournisseurs de technologies, aux assurances santé et mutuelles, ainsi qu'aux établissements de soins, concernés par les enjeux liés à l'e-santé.

Contact : redaction@mindhealth.fr