L'Agefi Hebdo
08/03/2018

Mise en conformité RGPD, un projet au cœur de la transformation digitale

Laurent Mader, *associé, Grant Thornton (photo haut),*
et Nicolas Rémy Neris, *avocat, Grant Thornton Société d'Avocats (photo bas)*

LE RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION des données) a été publié le 24 mai 2016 avec une date d'entrée en vigueur fixée au 25 mai 2018 : nous observons que de nombreux établissements bancaires en ont repoussé les préparatifs de mise en place jusqu'au premier trimestre 2018. Comme dans tout chantier réglementaire, la composition de l'équipe projet est la condition sine qua non de réussite. Les organisations mettent en œuvre leur projet au travers d'une approche souvent « classique » comprenant une phase de diagnostic aboutissant à une analyse d'écart entre l'existant et les exigences à atteindre, et une phase de mise en œuvre des adaptations de la conformité identifiées lors de l'analyse d'écart. Qui dit classique ne signifie pas pour autant que le choix des parties prenantes au projet n'est pas essentiel. Cette équipe doit réunir un nombre élargi de fonctions et métiers. Il est illusoire d'imaginer que la mise en conformité puisse être réalisée sans un projet intéressant les services informatique, juridique et *risk management*. Cette liste doit être élargie au regard de l'organisation de l'entreprise et des services concernés. Parfois, nous observons une première intention de cantonner la mise en conformité à la sécurité informatique, ce choix est rapidement abandonné par souci d'efficacité.

Lors du lancement, nous pouvons observer une réticence des participants internes. S'agissant de la phase de diagnostic, il est essentiel de rassurer l'équipe sur ses objectifs. Les sponsors doivent faire preuve de pédagogie pour expliquer ce qu'est une donnée à caractère personnel et le niveau de granularité attendue à ce stade. L'enjeu n'est pas tant de « traquer » la donnée en elle-même ou de réaliser le registre des traitements, que de rentrer dans une réflexion interne sous l'angle « organisationnel et métier ». C'est le seul levier efficace pour s'assurer que cette réforme intègre l'ADN des organisations qui la mettent en place. Il s'agira de déterminer dans chaque service et métier la nature des données personnelles traitées, la sécurité des outils et les tiers éventuels opérant un traitement. On privilégiera une approche macroscopique de la donnée personnelle afin de prendre du recul sur le fonctionnement de l'organisation auditée et les utilisations des données.

« PRENDRE DU RECUL SUR LE FONCTIONNEMENT DE L'ORGANISATION ET LES UTILISATIONS DES DONNÉES »

Une autre réaction souvent observée est la crainte de voir le projet de conformité empiéter sur le temps et, par ricochet, la « productivité » des équipes qui voient le RGPD comme un frein. D'expérience, le projet permet au contraire la prise de conscience par l'organisation de son patrimoine informationnel, une uniformisation des bonnes pratiques, la création d'une conscience collective dans l'importance de la *data* et l'impérieuse nécessité de sa sécurisation.

VALORISER LE LIEN CLIENT

Durant la phase de mise en œuvre, l'équipe projet doit être relayée de manière très opérationnelle dans les différents services et métiers concernés. Lors de cette phase, la formation des collaborateurs devra être réalisée. L'approche devra être valorisée et soutenue par le top management de l'organisation : l'appropriation du sujet par les collaborateurs est à la fois un gage de succès et de relais efficace pour l'équipe et un gage de pérennité de la conformité. Ainsi, déployer un projet de conformité RGPD, c'est accompagner le changement d'ADN de l'organisation, accélérateur de la transformation digitale, dans un projet de gouvernance des directions générales, de gestion des risques financiers et d'image, et de tous les impacts économiques qui en découlent. C'est enfin un projet de gestion du risque pénal des dirigeants.

Alors que la majorité des dernières réglementations a eu pour conséquence de contraindre davantage les activités des établissements de crédit, au point parfois de les écarter de leur fonction d'origine, et de distendre le lien client, expliquer la conformité RGPD est l'occasion de communiquer et valoriser cette relation pour, in fine, renforcer la confiance dans la transparence. C'est très précisément l'essence même du texte européen, dont le but ultime est d'assurer la sécurité de l'économie numérique, tout en posant les règles impératives garantissant la vie privée de chacun dans les mutations en cours.