La facture salée que le GDPR prépare aux entreprises

Le 25 mai 2018, les entreprises devront appliquer le GDPR, le règlement européen sur la protection des données. Cette loi unique à l'échelle des pays de l'Union européenne en matière de protection des données personnelles de citoyens (qui disposeront alors de plus de contrôles) entrainera de nouvelles obligations et contraintes pour les entreprises européennes comme non européennes qui seront toutes soumises au même règlement. Elles devront s'assurer de la sécurisation des données, par la «pseudonymisation» et leur chiffrement, et en assurer la confidentialité et l'intégrité, notamment.

En cas de défaillance ou d'attaque, les organisations devront en alerter les autorités compétentes dans les 72 heures après avoir pris connaissance de l'incident (une attaque informatique, une fuite de données, par exemple). Mais aussi les personnes directement concernées (un vol de numéro de carte bancaire…) si les données sont exploitables (non chiffrées en l'occurrence).

Les organisations seront entièrement responsables de la chaîne de traitement des données et, à ce titre, devront s'assurer de la garantie apportée par les sous-traitants et leurs éventuels fournisseurs. Les entreprises de plus de 250 salariés devront également tenir un registre des activités de traitement effectué. Cela implique la nomination d'un délégué à la protection des données (DPO) pour les firmes traitant de grandes quantités de données (ou ayant de nombreux clients consommateurs).

Une conformité à 30 millions d'euros

Les organisations qui ne se mettront pas en conformité avec le GDPR prendront le risque de s'exposer à une amende de 20 millions d'euros ou 4% de leur chiffre d'affaires annuel mondial. La protection des données n'est plus seulement technique, elle fait intervenir la gestion du risque.

Une gestion coûteuse que le cabinet Sia Partners évalue à 30 millions d'euros en moyenne pour un groupe du CAC40, selon des chiffres rapportés par *Les Echos*. Avec d'énormes disparités selon les secteurs. Pour les banques et assurances, la facture pourrait s'élever à 100 millions d'euros en moyenne et 35 millions pour les autres entreprises s'adressant aux consommateurs. Celle des fournisseurs des organisations se limitera à 11 millions.

Un coût justifié par la mise à niveau des systèmes informatiques laquelle s'élèverait jusqu'aux deux-tiers du coût de l'application du nouveau règlement, selon le cabinet de conseil en gestion qui a appuyé son étude sur une série d'entretiens de responsables, de données publiques et de missions réalisées par ses consultants. Aux frais propres à l'IT s'ajoutent le recensement des données concernées et l'analyse des risques liés, ainsi que la désignation d'un DPO et organiser les équipes et structures en conséquence.

75% des entreprises non prêtes

Un chantier important, voire colossal pour les organisations qui ne disposent pas nécessairement de la culture des mises en conformité. Et elles sont nombreuses à appréhender les difficultés de mise en œuvre du nouveau règlement. Selon une étude du Ponemon Institute menée pour Citrix auprès de 4□000 professionnels de l'informatique et de la sécurité, 74% d'entre eux déclarent que le GDPR aura un impact significatif et négatif sur leurs opérations commerciales. Et si 67% des répondants sont conscients de l'arrivée du règlement européen, seulement la moitié commence à s'y préparer.

Des chiffres corroborés par une autre étude réalisée par Vanson Bourne pour l'éditeur de solutions de sécurité Varonis. Selon les 500 décideurs informatiques interrogés au Royaume-Uni, en Allemagne, en France et en Amérique du Nord, 75% des entreprises rencontreront des difficultés à se préparer pour l'échéance de mai 2018 (74% pour les entreprises françaises). Et parmi les 58% des organisations qui déclarent avoir procédé à une évaluation ou un audit pour identifier les personnes ayant accès aux données en interne, 69% reconnaissent avoir identifié au moins un cas d'accès trop permissif aux informations d'identification personnelle. Enfin, 55% avouent avoir des difficultés à pouvoir appliquer le « droit à l'oubli » (article 17 du GDPR).

Selon Varonis, ce sont les entreprises du secteur public qui risquent d'avoir le plus de mal à se conformer à la nouvelle réglementation. Seules 26% disposent d'un budget dédié contre 41% dans le secteur privé. *« La conclusion la plus inquiétante est qu'une entreprise sur quatre ignore où résident ses données sensibles »*, déclare Christophe Badot, directeur général France de Varonis.

Lire également
GDPR : pas de portabilité des données sans API, avertit un collectif
Florian Douetteau, Dataiku : « Le GDPR va remodeler les applications Big Data »
CISPE, lobby européen du Cloud, publie un code de conduite conforme GDPR