L'ARGUS de l'assurance

PAYS :France
PAGE(S) :46,47
SURFACE :131 %
PERIODICITE :Hebdomadaire

RUBRIQUE :Analyse
DIFFUSION :10624
JOURNALISTE :Sanaa Nouiri

► 8 décembre 2016 - N°7486

[ANALYSE]

Règlement européen – Protection des données personn elles

Data, la course co ntre la montre est lanc ée

Élément structurant pour le tissu économique en général et celui des assureurs en particulier, le règlement européen sur la protection des données est à l'aube de son application, prévue pour le printemps 2018.

Avec l'entrée en vigueur en mai 2016 du Règlement européen sur la protection des données à caractère personnel [1], les entreprises concernées sont, désormais, en ordre de marche pour une mise en conformité qui doit intervenir d'ici le 25 mai 2018. Mais force est de constater que la tâche n'est pas aisée tant l'impact des nouvelles obligations est important sur l'entreprise, son organisation et ses méthodes de travail. Or, ce règlement est le corollaire de l'évolution actuelle du *business model* classique des entreprises, qui tend à reposer de plus en plus sur les possibilités offertes par la donnée, autrement dit « la *data* ». En effet, avec l'explosion de l'économie collaborative, l'utilisation de nouveaux composants informatiques non encore maîtrisés, l'expansion continue du marché du *big data* et des objets connectés, la révolution *blockchain* et finalement la digitalisation de la société dans son ensemble, la valeur économique de la *data* ne semble, aujourd'hui, plus à démontrer.

Ainsi, la réglementation applicable en la matière ne doit surtout pas être négligée. D'autant plus que le Règlement européen prévoit des sanctions pouvant atteindre 4 % du chiffre d'affaires mondial pour une entreprise, notamment en cas de violation des principes de base d'un traitement, comme le non-respect des règles à suivre en matière de recueil du consentement et de communication des nouveaux droits aux personnes concernées. Il est , ainsi, possible d'identifier 6 chantiers de mise en conformité fondamentaux que devra mener toute entreprise (voir ci-contre).

Bien gérer le transfert des données des assureurs

Pour l'entreprise d'assurance et ses sous-traitants, il s'agit de savoir comment interpréter et apprécier les nouvelles obligations édictées par le règlement européen ? Quels changements organisationnels et quelles évolutions des systèmes d'informations et des processus sont à prévoir ? En premier lieu, un point essentiel de la nouvelle réglementation est à retenir : cette réforme vise d'abord à renforcer la protection des données à caractère personnel de tout individu, qu'il s'agisse d'un collaborateur, d'un client ou même d'un simple prospect de l'entreprise.

Ensuite, il paraît primordial pour l'assureur de parfaitement apprécier le champ d'application de cette nouvelle réglementation (filiales, prestataires, coresponsables de traitement, etc.). De plus, au-delà du périmètre *stricto sensu* de la donnée à caractère personnel, l'entreprise doit aussi se

L'ARGUS de l'assurance

PAYS :France
PAGE(S) :46,47
SURFACE :131 %
PERIODICITE :Hebdomadaire

RUBRIQUE :Analyse
DIFFUSION :10624
JOURNALISTE :Sanaa Nouiri

► 8 décembre 2016 - N°7486

concentrer sur une dimension plus opérationnelle, à savoir les traitements métiers qu'elle opère directement ou qu'elle délègue à des sous-traitants conformément à sa politique d'externalisation. Une catégorie de traitements préoccupe davantage les régulateurs européens – la Cnil en France – et *a fortiori* les assureurs : le transfert de données, en particulier lorsque ce transfert est à destination d'acteurs situés en dehors de l'Union européenne ou de pays tiers n'offrant pas les garanties légales de protection suffisantes.

Il semble que la plupart des entreprises d'assurance concernées initient, en ce dernier trimestre 2016, leur programme d'application du Règlement européen, en phase de cadrage pour certaines ou en phase de démarrage, voire de déploiement pour d'autres : la course contre la montre est donc désormais lancée.

Dynamisme concurrentiel

Au-delà d'un projet de mise en conformité, il s'agit pour toute entreprise d'en tirer profit pour lancer un long processus de revalorisation de la *data* au sein de son organisation. La *data* représente une part essentielle du capital de l'entreprise qu'elle doit régulièrement tenir à jour, vérifier, optimiser et protéger. En effet pour l'entreprise d'assurance, la donnée est une valeur inestimable. Elle est le fruit de recherches, de collectes, d'opérations mathématiques et statistiques, parfois de très haute volumétrie comme le *big data*, qui permet à des entreprises, telles que les banques ou les organismes d'assurance, d'en tirer des informations décisionnelles, de créer un avantage concurrentiel, voire de s'ouvrir de nouveaux marchés, jusque-là inconnus ou inaccessibles. Encore faut-il que la donnée soit de bonne qualité, à jour et protégée des risques de vol, d'altérations ou des modifications criminelles ou par négligence.

■ SANAA NOUIRI ET BENJAMIN NAHOUMOVITCH, *MANAGERS* EN *RISK MANAGEMENT* ET EXPERTS EN *DATA COMPLIANCE*, OPTIMIND WINTER

1. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

À RETENIR

■ L'importance économique de la *data* doit conduire l'industrie de l'assurance à se mettre en conformité avec le Règlement européen sur les données personnelles sous peine de paralysie de ses activités.

PAGES COORDONNÉES PAR JÉRÔME SPERONI

6 CHANTIERS FONDAMENTAUX

1. La sensibilisation et la communication
Formation et sensibilisation des acteurs internes. Élaboration d'une communication licite et transparente à destination des personnes concernées.

2. La gouvernance
Définition et déploiement du système de gouvernance dédié au Règlement européen au sein des entreprises. Désignation d'un DPO (*data protection officer*) et mise en place d'une organisation permettant un travail collaboratif entre les différentes directions concernées.

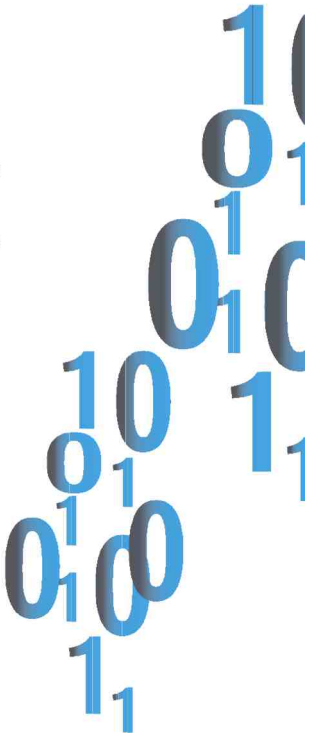
3. Les normes et contrôles
Documentation des nouvelles règles méthodologiques, comme l'analyse préalable des risques sur la vie privée, la gestion de crise en cas de violation ou encore les politiques de protection et de sécurité des données. Déploiement des plans de contrôles permanents et périodiques au sein des nouveaux processus liés au règlement européen (chez le responsable de traitement et ses sous-traitants).

4. Le cadre contractuel
Sécurisation et mise en conformité des engagements contractuels de l'entreprise avec ses fournisseurs, collaborateurs, clients et prestataires (conventions d'externalisation et règles d'entreprises contraignantes : *binding corporate rules*).

5. Les métiers et systèmes d'information
Documentation des nouveaux processus métiers et mise en œuvre des évolutions techniques et fonctionnelles des systèmes d'information afin de répondre à l'exercice des nouveaux droits des personnes concernées (accès, rectification, cloisonnement, suppression, etc.). Mise en place et alimentation d'un registre des activités de traitements.

6. Les mesures de sécurité
Définition et application de mesures techniques et de garanties appropriées assurant la sécurité des données à caractère personnel. Il s'agit principalement d'opérations d'anonymisation, de pseudonymisation, de chiffrement appliquées sur les données structurées ou non.

SOURCE : OPTIMIND WINTER.



L'ARGUS de l'assurance

PAYS : France
PAGE(S) :46,47
SURFACE :131 %
PERIODICITE : Hebdomadaire

RUBRIQUE : Analyse
DIFFUSION :10624
JOURNALISTE : Sanaa Nouiri

► **8 décembre 2016 - N°7486**

GRANDEDUC/GETTY IMAGES/ISTOCKPHOTO