

Respect du RGPD : l'heure tourne



Respectez-vous les obligations du règlement sur la protection de données ?

Les effets du règlement général sur la protection des données pourraient se révéler dévastateurs pour votre entreprise : il est urgent que les dirigeants comprennent les répercussions de cette nouvelle réglementation et les moyens de se mettre en conformité

Dans les entreprises, on commence à se rendre compte que le règlement général sur la protection des données (RGPD) entraîne un changement de paradigme dans la gestion des données à caractère personnel des personnes concernées au sein de l'UE, sans trop savoir quelle approche adopter.

Le défi actuel n'est pas tant d'éviter d'enfreindre la nouvelle réglementation, en vigueur à partir de mai 2018, que de savoir comment se prémunir contre les éventuels préjudices financiers et les atteintes à la réputation qui s'ensuivraient.

L'amende prévue, jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial (le montant le plus élevé étant retenu) pour non-respect du RGPD, galvanise les efforts. Il n'en reste pas moins que la mise en conformité s'avère difficile pour beaucoup : il convient, pour arriver à bon port, de définir sa feuille de route et de choisir le bon partenaire.

Mise en conformité avec le RGPD

Richard Hogg, responsable mondial des offres liées au RGPD et à la gouvernance chez IBM Cloud, fait remarquer que les entreprises, à différents stades du projet, peinent à évaluer toutes les ramifications des nouvelles règles et les étapes à entreprendre.

« Le RGPD porte sur toutes les données à caractère personnel des personnes concernées qui comprennent aussi bien vos employés que vos clients externes. Les réglementations sur la confidentialité des données dans les 28 états de l'UE ont durci les obligations relatives aux données à caractère personnel. Vous devez savoir quelles données sont en votre possession, où elles se trouvent, et comment elles sont traitées, sécurisées et protégées », explique Richard Hogg.

Les réglementations sur la confidentialité des données dans les 28 états de l'UE ont durci les obligations relatives aux données à caractère personnel. Vous devez savoir quelles données sont en votre possession, où elles se trouvent, et comment elles sont traitées, sécurisées et protégées



Objectif mai 2018 : le compte à rebours a commencé. Les entreprises doivent préparer dès maintenant leurs plans pour respecter en temps voulu les règles sur les demandes d'accès des personnes concernées et le droit à l'effacement

Dans l'UE, les personnes concernées ont de nouveaux droits. Par exemple, si un client veut mettre fin à une relation commerciale, il peut exercer son « droit à l'effacement » qui se traduit par la suppression de toute donnée à caractère personnel le concernant.

Il peut aussi demander à ce qu'une entreprise ou un organisme lui communique les données à caractère personnel détenues à son sujet, gratuitement et dans le délai d'un mois. Le droit à la portabilité dispose que les données sont facilement transférables à un nouveau fournisseur. De plus, le RGPD impose une stricte qualité des données.

Les entreprises et organismes doivent recueillir le consentement explicite des personnes concernées pour le traitement de leurs données. La transparence des données est essentielle ; leur sécurité et leur confidentialité sont vitales. En cas de violation des données à caractère personnel, l'entreprise doit signaler l'incident dans les 72 heures à l'autorité de contrôle compétente et, éventuellement, à la personne concernée.

Rôle du sous-traitant

Certes, beaucoup feront appel à un prestataire de services Cloud pour répondre aux défis du RGPD. Ils n'en seront pas pour autant dégagés de leur responsabilité de respect du règlement, obligation qui continue de relever de l'entreprise en tant que responsable du traitement, et non du sous-traitant.

Toutefois, le recours à un prestataire de services Cloud peut sans aucun doute faciliter la préparation et réduire la charge de travail.

« Pour les entreprises, un des plus grands défis réside dans leur méconnaissance des données personnelles en leur possession, disséminées entre plusieurs systèmes, de leur provenance et des voies qu'elles empruntent pendant le traitement », développe R. Hogg.

Pour apporter une réponse à ces défis, IBM Cloud propose d'entreprendre une étude d'impact sur la vie privée ou EIVP, aussi connue sous son acronyme anglais PIA (Privacy Impact Assessment), afin de produire le registre des activités de traitement exigé au titre de l'article 30 du RGPD.

« Une EIVP participe à la traçabilité des données, elle aide à en déterminer les catégories, les modes de traitement et le recueil du consentement. Elle couvre l'ensemble de l'entreprise et repère les éventuelles lacunes par rapport aux obligations du RGPD », poursuit R. Hogg.

Quelques semaines suffisent à mener une analyse EIVP. Ensuite, IBM Cloud peut vous aider à migrer vos données vers sa plateforme et faciliter votre mise en conformité avec le RGPD en classant et en protégeant les données.

Accélérer la mise en conformité

Les outils d'IBM permettent d'accélérer la cartographie de haut niveau des données afin d'identifier celles qui présentent un risque de violation du RGPD. Ces outils partent de la base pour rechercher des types de données prédéfinis, et cataloguer les données présentes.

« Vous pouvez recenser les données obsolètes et les supprimer, ainsi que déterminer s'il vous faut le consentement explicite des personnes concernées pour traiter leurs données », explique R. Hogg.

IBM Cloud peut aider les entreprises à repérer où se trouvent leurs données, en ligne ou sur site, et accompagne le processus de découverte et de cartographie lié à la préparation au RGPD.

« Les entreprises pourront faire le choix de transférer davantage de données dans le Cloud à l'avenir. IBM Cloud les accompagne dans le déploiement de l'infrastructure



Le RGPD n'accorde que 72 heures pour signaler une violation. En entreprise, le processus de découverte dure généralement 150 jours. IBM Cloud vous aide à tenir le délai grâce à ses fonctions étendues de surveillance

nécessaire pour un traitement des données sécurisé et respectueux de la vie privée. Il met à leur disposition toute la richesse de ses fonctions de confidentialité, de sécurité et de protection des données », ajoute R. Hogg.

En cas d'accès non autorisé, IBM Cloud propose un service de gestion des incidents à la demande pour découvrir la source du problème.

« Le RGPD n'accorde que 72 heures pour signaler une violation. En entreprise, le processus de découverte dure généralement 150 jours. IBM Cloud vous aide à tenir le délai grâce à ses fonctions étendues de surveillance », conclut R. Hogg.

Cliquez [ici](#) pour en savoir plus sur l'évaluation de la préparation au RGPD ou parlez à un revendeur Cloud de la mise en conformité RGPD. ■

Clause de non-responsabilité: *il incombe aux clients de se mettre en conformité avec les diverses lois et réglementations applicables, notamment le Règlement général sur la protection des données de l'Union européenne. Il revient aux clients, et à eux-seuls, d'obtenir des avis éclairés auprès d'un conseil juridique compétent pour connaître et interpréter les lois et réglementations pouvant avoir des effets sur leurs activités, et savoir quelles mesures prendre pour s'y conformer. Les produits, services et autres fonctionnalités décrits dans le présent article ne conviennent pas dans toutes les situations des clients et leur disponibilité peut être limitée. IBM ne fournit pas de conseils juridiques, comptables ou d'audit, et ne déclare ni ne garantit que ses services ou ses produits assureront aux clients la conformité à la législation ou la réglementation en vigueur.*

IBM Cloud aide les entreprises à migrer les données qu'elles détiennent, en prédefinisant des types de données et en les cataloguant pour plus de transparence et un traçage facilité

