Une bonne visibilité sur les données dans le Cloud

JOKERPRO/GETTY

Des accélérateurs SaaS multicloud pour préparer la conformité au RGPD

Les entreprises doivent absolument avoir une vue très claire, et globale, de toutes les données personnelles qu'elles détiennent pour garantir la conformité avec le Règlement général sur la protection des données et éviter une lourde amende

Nombre d'entreprises sont confrontées à la difficulté d'avoir à gérer des données personnelles résidant dans divers environnements en Cloud. Lorsque le Règlement général sur la protection des données (RGPD) entrera en vigueur en mai 2018, les entreprises devront être en mesure de se conformer à ses dispositions en matière de gouvernance des données personnelles, et de démontrer qu'elles respectent la confidentialité et assurent la sécurité des données personnelles.

Les entreprises doivent pouvoir cartographier les données personnelles afin de savoir où elles se situent et comment elles sont traitées. Elles doivent également les assortir de droits d'accès en mettant en place des pistes d'audit pour établir leur conformité à la réglementation. Dans le cadre de la pratique recommandée de protection intégrée de la vie privée, les données doivent être chiffrées et, le cas échéant, masquées pour éviter toute ré-identification des personnes concernées. Tout incident de sécurité doit en outre être signalé dans les 72 heures.

Contrôle des données

Le contrôle transparent des données est vital pour se conformer aux dispositions du RGPD et empêcher que les activités de traitement des données enfreignent la réglementation. L'entreprise encourt une amende pouvant aller jusqu'à 20 millions d'euros ou 4 % de son chiffre d'affaires global, le montant le plus élevé étant retenu.

Il est impératif que les entreprises aient une bonne visibilité et une vue d'ensemble de la sécurisation des données personnelles pour préparer leur mise en conformité avec le RGPD, et les accélérateurs SaaS (software-as-a-service) de préparation au RGPD peuvent rendre ce processus plus rapide.

Quel que soit l'endroit où les données sont physiquement stockées, l'entreprise reste responsable de leur traitement. C'est elle qui a la responsabilité ultime en cas de violation du RGPD, et elle doit par conséquent avoir une visibilité complète de toutes les données hébergées dans le Cloud ou administrées par des sous-traitants. Il est nécessaire de mettre en place des dispositifs de sécurité pour le suivi et le chiffrement des données, même si un sous-traitant affirme offrir une sécurité intégrée dans le Cloud.

Selon Ravi Srinivasan, Vice-président stratégie et gestion des offres chez IBM Security : « De plus en plus d'entreprises gèrent leurs activités dans un environnement multicloud et se retrouvent sur la sellette en tant que responsables de traitement. Elles doivent prendre en compte les parties prenantes et les organismes de réglementation, et si elles veulent rester sur le marché du numérique, il leur fait superviser la sécurité et la confidentialité dans un environnement multicloud. »

Une préparation en trois étapes

La démarche recommandée par IBM Security pour la mise en conformité avec le RGPD comporte trois éléments.

« La préparation au RGPD dans un environnement multicloud comprend trois étapes : trouver les données et les risques associés, sauvegarder l'accès aux données qui est utilisé et exposé à des risques, et être en mesure de réagir à un incident tel qu'une alerte ou une violation », déclare Ravi Srinivasan.

Le contrôle transparent des données est vital pour se conformer aux dispositions du RGPD et empêcher que les activités de traitement des données enfreignent la réglementation, l'entreprise encourant une amende pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires global, le montant le plus élevé étant retenu

Les entreprises qui utilisent un environnement hybride ou multicloud et sont confrontées à ces difficultés pourront tirer parti des offres d'accélérateurs SaaS multicloud d'IBM Security pour se mettre en conformité avec le RGPD. Ces accélérateurs peuvent être déployés sur site, dans le Cloud IBM ou dans d'autres environnements du Cloud tels qu'Amazon Web Services, Microsoft Azure, Google Cloud et Oracle Cloud.

Dans la mesure où les entreprises adoptent de plus en plus des environnements multicloud, il est crucial qu'elles puissent identifier les données à caractère personnel, où qu'elles résident, ainsi que tous les risques correspondants, et IBM apporte des solutions à ces entreprises.

IBM Guardium trouve les données personnelles dans les Cloud tiers et offre toute une série de fonctionnalités, depuis la détection et la classification jusqu'à la création de rapports axés sur la conformité au RGPD, en passant par l'évaluation de la vulnérabilité, la surveillance et l'alerte.

« Les entreprises veulent continuer à utiliser les données dans leurs activités quotidiennes. IBM Guardium permet de suivre et chiffrer ces données, de sorte que les entreprises peuvent les utiliser dans le fonctionnement courant de leurs activités au sein d'un environnement multicloud, tout en préparant dans le même temps la mise en conformité avec le RGPD », explique Ravi Srinivasan.

En tant que responsable du traitement, l'entreprise peut prouver qu'elle a le contrôle sur les données personnelles qu'elle détient et qu'aucun tiers malintentionné ne peut y accéder

Cartographier l'accès aux données

En tant que responsable du traitement, l'entreprise peut prouver qu'elle a le contrôle sur les données personnelles qu'elle détient et qu'aucun tiers malintentionné ne peut y accéder.

En cartographiant l'accès aux données jusqu'aux départements de l'entreprise qui les possèdent et les utilisent, les décideurs peuvent changer leurs processus en cas de besoin pour se mettre en conformité avec le RGPD.

IBM Guardium trouve et classe les données personnelles dans les Clouds tiers, en assure le suivi et les chiffre pour une transparence maximale

VEGE/ADOBE

Les solutions Agile 3 d'IBM permettent de cartographier pour chacun de ces départements les risques associés aux données afin de gérer des règles d'accès ciblées. Elles n'empêchent pas de continuer à collecter et à utiliser les informations, mais en masquent éventuellement certains éléments. Par exemple, les préférences personnelles contenues dans un message électronique peuvent être masquées de telle sorte que l'entreprise puisse quand même utiliser les données collectées.

« Les départements de l'entreprise peuvent modifier les processus pour se préparer au RGPD. Grâce à la vue globale que nous apportons, le projecteur est braqué sur ces données pour que l'entreprise puisse modifier ses pratiques métiers. Si nécessaire, elle peut décider de restreindre totalement l'accès pour respecter la disposition du RGPD relative à la gouvernance des identités », explique Ravi Srinivasan.

Avec un délai de seulement 72 heures pour déterminer l'étendue d'une éventuelle violation et notifier l'organisme de réglementation ainsi que les personnes concernées, il est vital de pouvoir localiser rapidement les données pour réagir au plus vite. Si l'entreprise chiffre déjà les données par défaut, elle ne sera peut-être pas tenue de notifier les personnes concernées, si l'autorité de réglementation estime que ce n'est pas nécessaire. IBM Resilient prend en charge les réponses accélérées aux incidents lorsqu'une entreprise doit respecter le délai prescrit par le RGPD et notifier les personnes concernées, ce qui permet de prendre les mesures nécessaires et de réagir rapidement aux incidents.

Analytique et sécurité

Les outils d'analytique d'IBM complètent ses outils de sécurité pour faciliter la préparation au RGPD.

La cartographie des données qui résident dans le Cloud améliore le catalogage, ce qui permet aux entreprises de savoir exactement où se trouvent les données personnelles.

« Le catalogue de gouvernance des informations ouvre une fenêtre sur les données utilisées dans des environnements multicloud et devient une source centrale fiable qui est vitale pour la préparation au RGPD », explique Richard Hogg, responsable mondial des offres liées au RGPD et à la gouvernance chez IBM Cloud.

IBM InfoSphere Optim Data Privacy fournit une série d'outils qui permettent aux entreprises de prendre les mesures nécessaires en prévision du RGPD pour l'ensemble des données structurées, par exemple en masquant les données à caractère personnel pour que les personnes concernées ne soient pas identifiables.

« Les entreprises veulent profiter des avantages liés au fait de posséder des informations exactes et fiables, de manière à être en bonne position pour créer une relation plus personnalisée et de confiance avec chaque client », déclare Richard Hogg.

Si vous voulez en savoir plus sur la manière dont les accélérateurs SaaS multicloud de préparation au RGDP peuvent être utiles à votre entreprise, consultez notre site Web ou contactez votre représentant IBM.

Pour en savoir plus sur le parcours de préparation au RGDP d'IBM, ainsi que sur nos fonctionnalités et offres liées au RGDP pour la prise en charge de votre parcours de mise en conformité, cliquez ici.

Les outils d'analytique d'IBM complètent ses outils de sécurité pour faciliter la préparation au RGPD. La cartographie des données qui résident dans le Cloud améliore le catalogage, ce qui permet aux entreprises de savoir exactement où se trouvent les données personnelles