Acronis

QUESTIONS FRÉQUENTES SUR LE RGPD

Questions fréquentes (FAQ)

Q : Qu'est-ce que le RGPD ?

R : Le règlement général sur la protection des données (RGPD) est une nouvelle législation de l'Union européenne (UE) qui renforce la protection des données privées des résidents de l'UE. Il remplace la mosaïque actuelle de législations nationales en matière de confidentialité des données à caractère personnel par un ensemble unique de règles directement appliquées par chaque État membre de l'UE.

Q : À quelle date le RGPD va-t-il entrer en vigueur ?

R : Le 25 mai 2018.

Q : Le RGPD s'applique-t-il uniquement aux entreprises établies dans l'Union européenne ?

R : Contrairement à une idée reçue, la réponse est non. Toute entreprise qui possède des clients dans l'Union européenne et qui collecte ou traite de toute autre manière les données à caractère personnel de ces clients est tenue de se conformer au RGPD.

Q : Quelle est la définition du terme « données à caractère personnel » dans le cadre du RGPD ?

R : On entend par « données à caractère personnel » toute information pouvant être utilisée pour identifier une personne. Cette définition est beaucoup plus large que la définition historique d'informations d'identification personnelles. Elle inclut le nom de la personne, l'adresse e-mail, les publications sur les réseaux sociaux, les informations propres à son identité physique, physiologique, culturelle ou génétique, les renseignements médicaux, les données de localisation, les coordonnées bancaires, l'adresse IP, les cookies, etc.

Q : Quel est le rôle exact du RGPD ?

R : Le RGPD règlemente la collecte, le stockage, le transfert et/ou l'utilisation de toutes les données à caractère personnel (opérations collectivement désignées par le terme « traitement ») appartenant à des résidents de l'UE. Toute organisation qui traite les données à caractère personnel de résidents de l'UE, y compris par le suivi de leur localisation ou de leurs activités (p. ex. au moyen de cookies de navigateur), relève de ce règlement, même si l'organisation chargée de ce traitement n'est pas physiquement établie dans l'UE.

Le règlement fait la distinction entre les « responsables du traitement » et les « sous-traitants ». Le responsable du traitement est l'organisme qui détermine les moyens et les finalités du traitement des données à caractère personnel. Tout tiers engagé par un responsable du traitement pour effectuer des opérations sur des données à caractère personnel (p. ex. un fournisseur de services de stockage dans le Cloud) est un sous-traitant.

Q : Quel est l'impact du RGPD sur la protection de la vie privée ?

R : Le RGPD renforce de façon significative la protection de la vie privée des résidents de l'UE et impose des obligations importantes aux entreprises, institutions ou individus qui traitent leurs données à caractère personnel. Dans le cadre du RGPD, les obligations des responsables du traitement de données à caractère personnel sont les suivantes :

- **Droits de la personne concernée :** Les résidents de l'UE peuvent exercer un meilleur contrôle sur leurs données à caractère personnel et demander notamment aux responsables du traitement de leur en fournir des copies, de les rectifier et de les supprimer totalement.
- **Preuve de la conformité :** Les responsables du traitement doivent mettre en œuvre des règles et des procédures adéquates de protection des données et conserver un registre détaillé sur leurs activités de traitement des données.
- **Notifications des violations de sécurité :** Les responsables du traitement doivent signaler toute violation de données aux autorités de contrôle locales compétentes et informer les personnes concernées.
- **Sanctions en cas de non-respect :** Les autorités de contrôle compétentes peuvent imposer de lourdes amendes aux organisations n'ayant pas respecté le règlement, dont le montant dépend de la gravité de la violation et des dommages subis.

Q : Le RGPD impose-t-il le maintien des données à caractère personnel dans l'UE ?

R : Pas exactement, mais il est difficile de transférer des données à caractère personnel à l'extérieur de l'UE (« transfert transfrontalier des données ») tout en respectant le RGPD. Plusieurs règles sont à prendre en compte. Premièrement, les transferts de données sont généralement autorisés vers tout pays destinataire figurant sur la liste des destinations dotées d'une sécurité « adéquate », autrement dit dont les mesures de protection de la confidentialité des données sont conformes aux exigences de l'UE. Dans certains cas, si le pays dans son ensemble n'est pas jugé adéquat, certains territoires ou secteurs peuvent l'être. Début 2018, la liste validée comprenait tous les pays de l'UE, trois pays hors UE appartenant à l'Espace économique européen (Islande, Liechtenstein et Norvège) et un petit nombre d'autres pays et territoires (Andorre, Argentine, Canada, Guernesey, Île de Man, Îles Féroé, Israël, Jersey, Nouvelle Zélande, Suisse et Uruguay).

Les transferts de données sont également autorisés vers des destinations recourant à des « règles d'entreprise contraignantes » conformes aux exigences de l'UE. Ces règles autorisent certaines entités légales au sein d'une entreprise et, dans certains cas, des groupes d'entreprises indépendantes engagées dans une activité économique conjointe, à transférer des données à caractère personnel. Pour ce faire, les règles d'entreprise contraignantes applicables devront être approuvées par une autorité de contrôle compétente et répondre aux critères de cohérence de l'UE.

D'autres destinations sont autorisées si elles respectent certains « codes de conduite » et « mécanismes de certification » généralement élaborés par une association professionnelle ou l'un de ses organes représentatifs, et uniquement sous réserve de leur approbation par les autorités de contrôle compétentes.

D'autres transferts de données sont également légitimes s'ils relèvent de l'article « Dérogations pour des situations particulières ». Il s'agit, par exemple, de tout transfert de données à caractère personnel répondant à l'une des conditions suivantes :

- La personne concernée a donné son consentement explicite et a été informée des risques potentiels.
- Le sous-traitant doit respecter une obligation contractuelle ou répondre à une requête légale.
- Le transfert est nécessaire pour des motifs d'intérêt public ou pour la sauvegarde des intérêts vitaux de la personne concernée
- Le transfert est nécessaire dans le respect des « intérêts légitimes » du responsable du traitement, sur lesquels ne prévalent pas les droits de la personne concernée. Le responsable du traitement des données doit évaluer les circonstances du transfert et prendre des mesures raisonnables pour protéger les données à caractère personnel

En un mot, il est généralement plus simple, moins risqué et moins coûteux pour la plupart des entreprises de ne pas transférer de données à caractère personnel à l'extérieur de l'UE et des pays de la liste approuvée. Le transfert de données à caractère personnel dans tout autre pays engendrera des frais et du travail supplémentaires ; vous devrez présenter aux autorités de contrôle compétentes toutes les mesures prises pour protéger ces données au titre du RGPD. Si vous décidez d'appliquer des règles d'entreprise contraignantes, des codes de conduite, des mécanismes de certification et/ou des dérogations pour des situations particulières afin de justifier d'autres types de transferts transfrontaliers de données, prenez conseil auprès de juristes compétents.

Q : Quel est l'impact du RGPD sur nos interventions en cas de violations de sécurité ?

R : Le RGPD oblige les responsables du traitement et les sous-traitants à déployer des systèmes de protection permettant de prévenir les violations de sécurité, d'en rechercher la présence par des mécanismes de surveillance et de les signaler si elles surviennent. Ils doivent mettre en œuvre et documenter les technologies, règles et procédures nécessaires pour assurer la prévention, la détection, le signalement et la notification des failles de sécurité. De nouvelles obligations de signalement plus strictes s'appliquent à tout incident, qu'il soit accidentel ou intentionnel, entraînant l'accès, le transfert, la modification ou la destruction de données à caractère personnel par des parties non autorisées.

Les incidents en matière de protection des données à caractère personnel peuvent être dus à des défaillances technologiques (p. ex. une défaillance de disque dur), à une erreur humaine accidentelle (p. ex. la suppression ou la corruption accidentelle de fichiers utilisateur par un employé de l'équipe informatique) ou à une compromission malveillante intentionnelle (p. ex. une attaque par ransomware, au cours de laquelle des cybercriminels chiffrent des données à caractère personnel et exigent une rançon pour les rendre accessibles).

Plus simplement, les responsables du traitement et les sous-traitants doivent tout mettre en œuvre pour identifier les incidents de sécurité affectant des données à caractère personnel, signaler ces incidents aux autorités de contrôle dans les 72 heures suivant la détection et, en cas d'altération, vol ou perte grave de données, prévenir rapidement les personnes concernées.

Q : Quels nouveaux droits des utilisateurs les responsables du traitement doivent-ils respecter ?

R : Le RGPD offre aux personnes concernées une visibilité et un contrôle renforcés sur l'utilisation de leurs données à caractère personnel par les responsables du traitement. Ces derniers doivent accéder (gratuitement) aux demandes des utilisateurs, notamment en leur indiquant les catégories de données à caractère personnel collectées, en leur fournissant une copie de ces données dans un format facilement accessible, en rectifiant toute erreur identifiée par les utilisateurs et en effaçant ces données sur demande (« droit à l'oubli »).

Q : Qu'est-ce qu'un délégué à la protection des données ? Les responsables du traitement et les sous-traitants doivent-ils en avoir un ?

R : Le délégué à la protection des données (DPD) est un employé ou un consultant que la plupart des responsables du traitement et des sous-traitants devront désigner comme principal responsable de la supervision de la conformité au RGPD. Les institutions publiques doivent satisfaire à une norme plus exigeante : presque toutes devront nommer un DPD. Les entreprises privées doivent nommer un DPD uniquement si elles traitent des volumes importants de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion, les convictions philosophiques, les données génétiques ou biométriques et/ou les condamnations pénales des personnes concernées.

Le DPD doit être un professionnel compétent rompu aux questions de conformité et doit posséder des connaissances spécialisées du droit et des pratiques en matière de protection des données. Son travail consistera à informer les responsables du traitement, sous-traitants et employés de l'entreprise de leurs obligations au titre du RGPD, à surveiller la conformité et à assurer la liaison avec l'autorité de contrôle.

Q : Que se passe-t-il si la non-conformité au RGPD d'une entreprise, en sa qualité de responsable du traitement, de sous-traitant ou des deux, est avérée ?

R : Les sanctions pour non-respect du RGPD sont sévères. Votre autorité de contrôle locale peut imposer une amende de 10 millions d'euros ou 2 % de votre chiffre d'affaires annuel, le montant le plus élevé étant retenu, pour les infractions de premier niveau. Il s'agit par exemple de l'absence de tenue de registres écrits, ou l'absence de mise en œuvre de mesures techniques et organisationnelles appropriées pour respecter les exigences de conformité. Les amendes peuvent s'élever à 20 millions d'euros ou 4 % de votre chiffre d'affaires annuel, le montant le plus élevé étant retenu, en cas d'infraction plus grave, comme une violation majeure de données et l'incapacité à protéger des données à caractère personnel contre le vol, l'altération ou la suppression.

Ces amendes peuvent être imposées aux responsables du traitement, tout comme aux sous-traitants. Les autorités de contrôle peuvent imposer une amende selon le principe de proportionnalité à un responsable du traitement et à ses sous-traitants, en évaluant la part de responsabilité de chacun dans la violation sur la base des mesures prises par chaque partie pour se mettre en conformité avec le RGPD.

Outre ces pénalités financières dissuasives, les entreprises qui ignorent ou sous-estiment délibérément leurs obligations de conformité au RGPD exposent leur réputation à un préjudice potentiel durable, ainsi qu'à des poursuites de la part de particuliers pour dommage « matériel ou non matériel » en cas de violation de leurs données à caractère personnel. Ces mêmes amendes et sanctions s'appliquent également aux sous-traitants tiers s'ils traitent des données à caractère personnel pour le compte d'une autre entreprise. La croissance du nombre de violations de données au cours de ces dernières années est exponentielle.

À titre d'exemple, selon les prévisions, le coût des attaques par ransomware passera de 800 000 dollars par an en 2015, à 8 à 10 milliards de dollars en 2018. Dès lors, rien qu'en considérant les manquements possibles au principe de signalement d'une violation, les risques de sanctions en cas de non-conformité sont énormes.

Q : La mise en conformité avec le RGPD semble complexe. Par quoi faut-il commencer ?

R : En sa qualité de fournisseur de solutions de protection des données, Acronis estime que la mise à niveau de votre infrastructure de stockage et de sauvegarde des données est une première étape indispensable sur la voie de la conformité au RGPD. Vous devez savoir exactement où sont stockées vos données, être en mesure de prévenir les violations telles que les attaques par ransomware et protéger les données en transit et au repos par un chiffrement robuste. Ces mesures de base auront des effets positifs et concrets sur votre situation de conformité au RGPD.

Mais vous ne devez pas compter uniquement sur nous pour déterminer votre stratégie de mise en conformité avec le RGPD. Demandez également l'avis de juristes et autres professionnels compétents.

Cette FAQ a été élaborée à des fins purement informatives. Elle ne constitue pas un avis juridique et ne doit pas être considérée ou interprétée comme tel. Par conséquent, n'agissez pas ou ne vous abstenez pas d'agir sur la base de son contenu, et recherchez plutôt l'avis de juristes ou d'autres professionnels.

Acronis

Pour plus d'informations, visitez notre site : **https://www.acronis.com/fr-fr/gdpr/**