Guide pratique sur la protection des données dans le cadre du RGPD :

Exigences et informations clés pour un partage d'e-mails et de fichiers en conformité avec les réglementations

AUTEUR : Tim Edgar chercheur principal à l'Institut Watson de l'Université Brown pour les affaires internationales et publiques

virtru

Qu'est-ce que le RGPD ?

Le règlement général sur la protection des données (RGPD) de l'Union européenne est le cadre de base assurant la protection des informations à caractère personnel des citoyens européens. Le RGPD énonce les exigences détaillées concernant la collecte, l'utilisation, le partage et la protection des informations personnelles.

Il remplace les règles en vigueur relatives à la protection des données de l'Union européenne (UE), qui se plaçaient déjà parmi les plus strictes à l'échelle internationale. Les anciennes règles de l'UE sur la protection des données faisaient l'objet d'une directive, ce qui signifie que les États membres de l'UE étaient tenus d'adopter une législation visant à rendre ces règles contraignantes. Le RGPD est un règlement, ce qui signifie qu'il s'applique directement et uniformément dans l'ensemble de l'UE et dans trois autres pays faisant partie de l'Espace économique européen : la Norvège, le Liechtenstein et l'Islande.

Le RGPD a été adopté en avril 2016 et est entré en vigueur le 25 mai 2018.

Même s'il couvre un large éventail de sujets liés à la confidentialité et à la protection des données, cet article se concentre principalement sur les dispositions du règlement relatives au chiffrement et au contrôle d'accès.

Qui est concerné par le RGPD ?

Ce règlement concerne toutes les entreprises ou entités qui proposent des biens et services dans l'UE (à des fins commerciales ou non), qui surveillent les comportements dans l'UE, ou qui proposent des biens et services ou surveillent les comportements en Norvège, au Liechtenstein et en Islande.

Le RGPD concerne bien plus d'organisations que les anciennes règles de l'UE sur la protection des données. Auparavant, l'application de ces règles dépendait du fait que l'entité soit « établie » dans l'UE. Le RGPD s'applique à l'échelle internationale.

Il s'applique aux « responsables du traitement » des données et aux « sous-traitants » des données. Le responsable du traitement des données correspond à l'entité (par exemple, une entreprise) qui détermine les fins, les conditions et les méthodes de traitement des données à caractère personnel. Le sous-traitant des données correspond à l'entité chargée du traitement réel des données à caractère personnel (comme un fournisseur de cloud ou autre service tiers). Une même organisation peut jouer le rôle de responsable du traitement et de sous-traitant.

Si je n'exerce pas mon activité professionnelle en Europe ou ne gère pas de données personnelles de citoyens européens, mon organisation peut-elle être concernée par le RGPD ?

Oui. Les règles sur la protection des données de l'Union européenne ont une influence partout dans le monde. L'UE facilite le transfert de données personnelles en dehors des pays européens si elle détermine que ces derniers assurent une protection de la confidentialité « équivalente » à celle fournie par l'UE. Par conséquent, nombre d'autres pays ont adopté des règles similaires pour protéger les informations personnelles de leurs citoyens :

- **Le gouvernement britannique a annoncé en juin 2016 qu'il adopterait une loi incluant le RGPD, malgré sa sortie de l'UE.**

- Plus de 100 pays ont adopté une loi relative à la protection des données reprenant tout ou partie des règles de l'UE sur la protection des données. Nombre d'entre eux sont susceptibles de mettre à jour leur loi en vue de l'adoption du RGPD par l'UE.

Quelles sont les données considérées comme des données à caractère personnel par le RGPD ?

Voici certains exemples :

- Nom
- Photo
- Adresse e-mail
- Adresse IP
- Informations bancaires ou autres informations personnelles
- Informations de santé
- Publications sur les réseaux sociaux
- Toute autre donnée permettant d'identifier une personne

Que se passe-t-il si j'ignore le RGPD ?

En cas de violation importante du règlement, les organisations peuvent recevoir une amende d'un montant maximal de 20 millions d'euros ou équivalent à 4 % du chiffre d'affaires annuel mondial, selon le montant le plus élevé. (Ces montants sont largement supérieurs aux pénalités antérieures prévues par les règles sur la protection des données de l'UE en cas de violation.)

Quelles sont les exigences techniques associées au règlement ? Quelle est l'utilité de Virtru dans ce contexte ?

Les solutions de gestion de l'accès et du chiffrement de Virtru facilitent le respect de la conformité au RGPD en apportant les quatre éléments suivants :

- Chiffrement côté client robuste et facile à utiliser pour les e-mails et les fichiers.
- Contrôle complet des clés de chiffrement client.
- Puissants outils de contrôle d'accès permettant aux organisations de garder le contrôle sur leurs données, quel que soit l'endroit où les fichiers et les e-mails sont créés, stockés ou partagés.
- Outils d'audit facilitant la création de rapports et la fourniture d'informations sur la date et le lieu où les utilisateurs ont accédé aux fichiers et aux e-mails, ou les ont partagés.

Chiffrement

Le RGPD inclut des exigences strictes en matière de sécurité, incluant le chiffrement, dans le cadre de son approche globale de la cybersécurité centrée sur les risques. Les organisations doivent évaluer le risque de perte de données et de violation de données, ainsi que déterminer les mesures techniques à adopter pour limiter ces risques, notamment la pseudonymisation et le chiffrement. Toute violation doit être signalée aux régulateurs dans les 72 heures et les personnes concernées par les données doivent en être informées « sans retard excessif », à moins que l'organisation prouve que les données étaient chiffrées.

Le RGPD exige expressément de considérer le chiffrement des données à caractère personnel comme une obligation générale d'adopter des technologies reflétant « l'état des connaissances » en matière de sécurité. Par conséquent, le chiffrement est effectivement obligatoire pour des nombreuses organisations et cas d'utilisation. Sachant que le chiffrement est une mesure de sécurité commune et que les risques liés à la cybersécurité augmentent, il est probable que les organismes de réglementation et les tribunaux estiment dans de nombreuses situations, voire la plupart d'entre elles, que la décision de renoncer au chiffrement constitue une violation du RGPD.

Dans un rapport publié en 2014 sur la protection des données et de la confidentialité dès la conception, l'Agence européenne chargée de la Sécurité des Réseaux et de l'Information (ENISA) a examiné le chiffrement de bout en bout et le chiffrement côté client. Le chiffrement côté client est généralement utilisé par les fournisseurs de services cloud pour protéger les données en transfert vers et à partir du fournisseur de cloud. Avec le chiffrement de bout en bout, les données sont stockées dans le cloud sous forme chiffrée, sans que les fournisseurs de cloud ne puissent y accéder.

Le rapport de l'ENISA indique notamment que les services comme le « courrier électronique » qui assurent les communications entre les utilisateurs finaux « doivent privilégier le chiffrement de bout en bout pour les communications entre les utilisateurs, c'est-à-dire que le chiffrement est ajouté à un point de terminaison utilisateur et qu'il est éliminé uniquement sur l'autre point de terminaison utilisateur, ce qui rend le contenu des communications inintelligible pour les tiers, y compris les fournisseurs de services ».

C'est précisément ce que propose Virtru. Les e-mails et les fichiers sont chiffrés sur le client pour protéger les données avant qu'elles ne quittent votre appareil. Bien que de nombreux services cloud (comme Gmail) mettent à disposition des canaux chiffrés pour la communication entre le client et le fournisseur de services cloud, le contenu reste disponible pour ce dernier. Cela augmente la vulnérabilité des données à caractère personnel, tant face aux violations qu'aux activités de surveillance par le gouvernement prévues par des lois comme le Foreign Intelligence Surveillance Act (FISA) aux États-Unis. Toutefois, si un client utilise Virtru, les données stockées par le fournisseur de services sont chiffrées de bout en bout. De cette façon, la norme de sécurité reflétant « l'état des connaissances » recommandée par le rapport de l'ENISA est respectée pour les e-mails.

Gestion des clés

Le RGPD prescrit l'adoption d'une approche basée sur les risques liés à la cybersécurité. Il exige que les organisations prennent des mesures techniques reflétant « l'état des connaissances », y compris le chiffrement, si nécessaire. Cette approche oblige implicitement les organisations à intégrer la gestion des clés dans le cadre de leurs politiques globales pour la protection des données à caractère personnel.

Ici encore, le rapport de l'ENISA apporte des informations utiles. Voici ce qu'il indique :

Bien que les fournisseurs de services souhaitent aider les utilisateurs à s'authentifier mutuellement afin d'établir un canal chiffré de bout en bout, il est préférable, du point de vue de la confidentialité, que les clés utilisées pour protéger la confidentialité et l'intégrité des données ne soient jamais mises à la disposition des fournisseurs de services, mais dérivées sur les dispositifs des utilisateurs finaux.

Le service de chiffrement de Virtru garantit que votre fournisseur de services cloud (comme Gmail) n'ait jamais accès aux clés de chiffrement utilisées pour protéger votre contenu. Avec son serveur clé client (CKS), Virtru offre également aux clients la possibilité d'héberger leurs propres clés de chiffrement. Les clés peuvent être géolocalisées et hébergées sur site, dans un cloud privé ou dans le cloud public, selon le choix du client. L'offre CKS fournit à l'entreprise le contrôle exclusif de ses clés de chiffrement. Aucun fournisseur de cloud ou autre tiers n'a accès aux clés non chiffrées.

Contrôle d'accès

Le RGPD inclut de nombreuses exigences relatives à la gestion des données personnelles allant au-delà de la sécurité reflétant « l'état des connaissances », y compris le chiffrement. Il met l'accent sur la responsabilité et la gouvernance des données. Il exige que les organisations prennent le contrôle des données personnelles qu'elles gèrent.

Les organisations doivent prouver qu'elles ont adopté des politiques et procédures assurant le contrôle des données à caractère personnel. Elles doivent utiliser des systèmes qui assurent la confidentialité dès la conception, c'est-à-dire qui protègent les données par défaut, et non après coup. Leurs systèmes doivent être en mesure de fournir aux personnes concernées par les données les droits que leur confère le RGPD, tels que les droits liés à l'expiration et à l'effacement.

Virtru fournit un hôte de fonctionnalités de contrôle d'accès qui permet aux organisations de respecter ces exigences. Les e-mails et les fichiers sont protégés à partir du moment où ils sont créés, puis tout au long de leur cycle de vie, quel que soit l'endroit où ils sont partagés. Les utilisateurs et les administrateurs déterminent qui peut accéder au contenu et pendant combien de temps.

L'accès peut être révoqué à tout moment, même une fois que les e-mails et les fichiers ont été partagés ou ouverts. Virtru propose également l'expiration automatique au bout d'une certaine période, permettant ainsi aux organisations d'appliquer des limites de conservation des données à caractère personnel. Le transfert d'e-mails ou de fichiers peut être audité, limité ou interdit.

Audit

Le RGPD met l'accent sur la responsabilité et l'audit des données. Les organisations doivent conserver des enregistrements permettant de démontrer qu'elles respectent les exigences du RGPD et mettre ces enregistrements à la disposition des régulateurs. Les organisations qui traitent des données personnelles à grande échelle ou des données particulièrement confidentielles doivent nommer un « délégué à la protection des données » de haut niveau pour appliquer les politiques de protection des données et de la confidentialité.

Les fonctionnalités de Virtru aident les organisations à prouver qu'elles prennent la conformité au sérieux. Les administrateurs peuvent contrôler l'accès au contenu protégé en temps réel. Ils peuvent consulter la date de transfert ou de partage des e-mails et des fichiers, ainsi que les utilisateurs qui y ont accès.

Virtru a breveté une technologie de recherche permettant aux administrateurs de rechercher du contenu chiffré archivé afin de répondre aux exigences légales et réglementaires en matière d'e-discovery et autres exigences.

Enfin, Virtru dispose d'outils de protection contre la perte de données (DLP) qui permettent aux administrateurs de définir des règles de protection automatique du contenu confidentiel, y compris les informations à caractère personnel, en avertissant les utilisateurs, en ajoutant le chiffrement, en envoyant des notifications aux administrateurs, et bien plus encore.

Exigences du RGPD et Virtru : résumé rapide

Le logiciel de protection des données de Virtru offre des fonctionnalités visant à aider votre organisation à respecter ces exigences en matière de partage d'e-mails et de fichiers :

Sujet	Exigences du RGPD	Fonctionnalités Virtru correspondantes
Chiffrement des e-mails et cloud basé sur les risques	Les responsables du traitement et les sous-traitants doivent « [mettre] en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » y compris le « chiffrement des données à caractère personnel », entre autres mesures de sécurité. *Art. 32. Voir aussi le préambule, ¶ 83, p. 51.*	Virtru offre un chiffrement des e-mails et cloud de bout en bout, utilisant un chiffrement AES 256 bits fort.
Sécurité reflétant l'état des connaissances	Les mesures techniques, y compris le chiffrement, doivent prendre en compte l'« état des connaissances », les coûts et la gravité du risque. *Art. 32*. D'après l'Agence européenne chargée de la Sécurité des Réseaux et de l'Information (ENISA), l'« état des connaissances » sur le chiffrement d'e-mail exige un système de sécurité de bout en bout.	Le chiffrement côté client de bout en bout proposé par Virtru correspond à la technologie de pointe du chiffrement d'e-mail.
Gestion des clés	Le RGPD n'inclut pas de règles spécifiques pour la gestion des clés, mais il exige que les mesures de sécurité technique tiennent compte de l'« état des connaissances ». L'ENISA a reconnu que les utilisateurs peuvent vouloir tirer parti des fournisseurs de services de chiffrement, tout en reconnaissant qu'il est préférable, du point de vue de la confidentialité, que les fournisseurs de services n'aient pas accès aux clés.	Virtru permet aux clients de gérer leurs clés via son serveur clé client (CKS), d'utiliser le serveur de clé sécurisé de Virtru ou un autre fournisseur de cloud.

Sujet	Exigences du RGPD	Fonctionnalités Virtru correspondantes
Réutilisation des données personnelles à d'autres fins	Si un responsable du traitement souhaite recourir à des exceptions permettant d'utiliser les données à caractère personnel à des fins autres que celles pour lesquelles elles ont été collectées, il doit tenir compte de « l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation ». *Art. 6(4).*	La sécurité de Virtru basée sur les objets permet aux administrateurs de définir des règles pour le partage d'informations, le contrôle des transferts et la révocation de l'accès.
Exception à la notification de violation	En général, les responsables du traitement doivent signaler les violations de données aux autorités dans les 72 heures, et aux personnes concernées « sans retard excessif ». Toutefois, les organisations ne sont pas tenues de signaler les violations aux personnes concernées par les données si ces dernières ont été rendues inintelligibles pour toute personne n'étant pas autorisée à y accéder à l'aide de mesures comme le chiffrement. *Art. 34(3).*	Le chiffrement robuste AES 256 bits de Virtru est de qualité militaire. À moins que le contenu chiffré et les clés ne soient endommagés, les informations restent inintelligibles pour les personnes non autorisées.
Confidentialité dès la conception et par défaut	Les responsables du traitement doivent tenir compte de la protection des données et de la confidentialité dans la conception de leurs systèmes, ce qui inclut des mesures techniques visant à garantir « par défaut » que seules les données à caractère personnel nécessaires sont traitées. Cette obligation s'applique à la quantité de données à caractère personnel collectées, à la portée de leur traitement, et à la durée de leur stockage et de leur accessibilité. *Art. 25(2)*	Virtru permet aux administrateurs de définir des règles pour le partage de données, de limiter ou d'empêcher le transfert d'e-mails ou de fichiers, et de définir l'expiration des données. Il inclut des fonctions de protection contre la perte de données pour avertir les utilisateurs, ajouter le chiffrement, envoyer des notifications aux administrateurs, etc.

Sujet	Exigences du RGPD	Fonctionnalités Virtru correspondantes
Contrôle d'accès	Le responsable du traitement doit s'assurer « que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée ». *Art. 25(2)*. En d'autres termes, les responsables du traitement doivent démontrer qu'ils peuvent contrôler à qui sont fournies les données à caractère personnel.	Les utilisateurs et les administrateurs déterminent qui peut accéder au contenu et pendant combien de temps. L'accès peut être révoqué à tout moment, même une fois que les e-mails et les fichiers ont été partagés ou ouverts.
Neutralité technologique	Le règlement exige que « la protection des personnes physiques devrait être neutre sur le plan technologique ». *Préambule ¶ 14, p. 9* En d'autres termes, l'obligation de protéger les données à caractère personnel ne devrait pas dépendre de la technologie utilisée par l'organisation (par exemple, stockage de données sur site ou dans le cloud).	Les e-mails et les fichiers sont protégés à partir du moment où ils sont créés, puis tout au long de leur cycle de vie, quel que soit l'endroit où ils sont partagés. Virtru ne dépend pas de l'appareil ou de la plate-forme utilisée.
Audit et conformité	Les données à caractère personnel ne peuvent être traitées que pour certains motifs légitimes (contrat, intérêts vitaux, intérêt public, entre autres) ou avec le consentement valable de la personne concernée. Le consentement doit être donné dans un langage clair et simple. Les conditions longues et formalistes des accords de service ne fonctionnent pas. Les organisations sont tenues de conserver des enregistrements comme preuve de leur conformité à ces règles et à d'autres règles.	Les administrateurs peuvent contrôler l'accès au contenu protégé en temps réel. Ils peuvent consulter la date de transfert ou de partage des e-mails et des fichiers, ainsi que les utilisateurs qui y ont accès. Les e-mails et les fichiers peuvent être classés en fonction de leur contenu afin de soutenir les actions de protection des données.

Sujet	Exigences du RGPD	Fonctionnalités Virtru correspondantes
Retrait du consentement	Le règlement précise qu'il doit être aussi facile de retirer son consentement que de le donner, et que l'organisation doit être en mesure de rendre effective la décision de la personne concernée par les données de retirer son consentement.	Virtru permet à un administrateur de rechercher des fichiers protégés par mot-clé (comme un nom ou un numéro d'identification) et permet de révoquer l'accès à tout moment, même lorsque les données ont été ouvertes ou transférées.
Effacement	Les personnes concernées par les données ont le droit de faire effacer les données lorsqu'elles ne sont plus pertinentes (communément appelé « droit à l'oubli »).	Il est possible de définir des règles qui révoquent l'accès aux données au bout d'un délai spécifique.
Conservation et expiration	Les organisations doivent spécifier les politiques prévoyant des limites de conservation des données à caractère personnel et veiller à ce que ces données soient effacées ou rendues inutilisables au bout d'un certain temps (expiration).	Il est possible de définir des règles qui révoquent l'accès aux données au bout d'un délai spécifique.

À propos de l'auteur

Timothy H. Edgar est un ancien responsable du renseignement et de la sécurité nationale, expert en cybersécurité, avocat spécialisé dans la protection de la confidentialité et militant pour les libertés civiles. Timothy Edgar a rejoint l'Union américaine pour les libertés civiles (ACLU) peu après les attentats terroristes du 11 septembre 2001 et a lutté pendant cinq ans au Congrès face aux abus dans la « guerre contre le terrorisme ». Il a quitté l'ACLU pour s'intéresser en interne à l'état de surveillance croissant des États-Unis. Il fait part de son témoignage dans le livre *Beyond Snowden: Privacy, Mass Surveillance and the Struggle to Reform the NSA*.

En 2006, Timothy Edgar est devenu le premier député de la communauté du renseignement pour les libertés civiles, ayant le rôle de conseiller du directeur des services de renseignement nationaux sous l'administration de George W. Bush. En 2009, après l'annonce du président Barack Obama sur la création d'un nouveau poste au Conseil national de sécurité spécifiquement dédié à la protection de la confidentialité et des libertés civiles du peuple américain, Timothy Edgar est entré à la Maison Blanche, où il a conseillé le président sur les questions de protection de la confidentialité dans la politique liée à la cybersécurité.

En 2013, Timothy Edgar a quitté le gouvernement pour intégrer l'Université Brown afin de lancer son programme de diplôme professionnel relatif à la cybersécurité. Aujourd'hui, il est chercheur à l'Institut Watson de l'Université Brown pour les affaires internationales et publiques. Timothy Edgar travaille également avec les entreprises pour les aider à surmonter les problèmes de cybersécurité. Il fait partie du comité consultatif de Virtru, qui offre un logiciel de chiffrement simple dédié aux entreprises et aux individus.

Timothy Edgar s'est entretenu avec Christiane Amanpour de CNN et il a été fait mention de son travail dans le *Wall Street Journal*, le *Los Angeles Times*, le *Guardian*, *Foreign Affairs* et *Wired*. Il participe en tant que rédacteur en collaboration à « *Lawfare: Hard National Security Choices* ». Timothy Edgar a travaillé en tant qu'assistant de la juge Sandra Lynch, à la Cour d'appel des États-Unis pour le premier circuit, et il est diplômé de la Faculté de droit de Harvard et du Dartmouth College.

N'hésitez pas à nous contacter afin de découvrir comment tirer profit de Virtru pour protéger vos e-mails et vos fichiers conformément au RGPD.
virtru.com/fr/contact-sales

Chez Virtru, nous permettons aux organisations d'exploiter leurs données en toute simplicité tout en gardant le contrôle, quel que soit l'emplacement où elles sont stockées et partagées. Notre portefeuille de solutions et d'outils, fondés sur notre plateforme de protection des données ouverte, régit les données tout au long de leur cycle de vie. Plus de 20 000 organisations font confiance à Virtru pour la sécurité des données et la protection de la confidentialité. Rendez-vous sur virtru.com/fr ou suivez-nous sur Twitter @virtruprivacy.