StorageCraft®

FAQ sur le RGPD

Q. Qui et que protège le RGPD ?

R. Le Règlement général sur la protection des données est la nouvelle loi exhaustive de l'Union européenne concernant la vie privée et la protection des données. Dans les grandes lignes, le RGPD protège les « données personnelles » des individus dans l'Espace économique européen (EEE). Le terme « individu » fait référence à un être humain ou à une personne physique, et non pas à une entité. StorageCraft est une entreprise B2B et la plupart des données personnelles auxquelles nous avons affaire sont liées à nos employés ou à nos entreprises partenaires, ou sont contenues dans les sauvegardes que nous traitons via nos produits et services cloud.

Q. Pourquoi le RGPD s'applique-t-il à StorageCraft alors que son siège se trouve aux États-Unis ?

R. Même si le siège de StorageCraft se trouve aux États-Unis, le RGPD s'applique généralement, que nous fournissons nos services à des clients (ou à leurs filiales) dans l'EEE, ou que nous fournissons des services via notre filiale irlandaise.

Q. Que signifie le terme « données personnelles » ?

R. Une « donnée personnelle » représente toute information pouvant être utilisée pour identifier une personne, que ce soit de manière directe ou indirecte. Il peut notamment s'agir d'un nom, d'un numéro de téléphone, d'une adresse postale, d'une adresse e-mail, d'une date de naissance, d'un numéro d'identification (numéro de permis de conduire, d'assurance ou de sécurité sociale) ou d'une photographie. Les données personnelles englobent aussi des informations d'identification qui semblent moins évidentes, notamment les adresses IP ou les noms d'utilisateur en ligne.

Q. Le numéro de téléphone et l'adresse e-mail professionnels d'une personne peuvent-ils être considérés comme des « données personnelles » ?

R. Oui. Le fait que ces informations soient d'ordre professionnel n'a pas d'importance. Si des informations peuvent être utilisées pour identifier quelqu'un, que ce soit de manière directe ou indirecte, ces informations sont des « données personnelles » et sont protégées par le RGPD.

Q. Qu'est-ce qu'un « accord sur le traitement des données » (ou avenant relatif au traitement des données) ?

R. Dans le cadre du RGPD, le « responsable du traitement » est la partie qui détermine la finalité et les moyens relatifs au traitement des données personnelles. Le « sous-traitant », quant à lui, traite les données personnelles pour le compte du responsable du traitement. Le RGPD exige que la relation entre le responsable du traitement et le sous-traitant soit régie par un accord écrit. Ledit accord doit inclure un certain nombre de conditions minimales obligatoires, notamment des « garanties suffisantes » montrant que le responsable du traitement a mis en œuvre des « mesures techniques et organisationnelles adaptées » concernant son traitement des données. Cet accord est généralement appelé « accord sur le traitement des données » (ATD) ou « avenant relatif au traitement des données ». On croit souvent à tort que dès que des données personnelles sont transmises d'une partie à une autre, un ATD est requis. Or, ce n'est pas le cas. Un ATD est requis uniquement dans le cas où un responsable de traitement transfère des données personnelles à un sous-traitant afin que ce dernier les « traite » pour et pour le compte du responsable de traitement. Autrement dit, si la partie A ne fournit pas de données personnelles à la partie B (que ce soit en lui y donnant l'accès ou en les lui transférant) afin que la partie B traite ces données personnelles pour la partie A, un ATD n'est pas nécessaire. Si la partie recevant des données personnelles ne traite pas ces données pour et pour le compte de la partie qui les lui a transférées, mais les traite à des fins licites qui lui sont propres (ex. : la partie B met en œuvre un contrat), un ATD n'est pas requis.

Q. Quelles sont les relations partenaires StorageCraft qui nécessitent un ATD ?

R. Le tableau ci-dessous résume les principales relations partenaires StorageCraft, indique si un ATD est requis et explique notre raisonnement :

Relation avec StorageCraft	Accord sur le traitement des données nécessaire ?	Explication
Revendeur à valeur ajoutée (VAR – Vendant des logiciels perpetuels)	Non	Les seules données personnelles que StorageCraft devrait recevoir de la part d'un VAR sont les noms et adresses e-mail des employés du VAR ou des employés de l'utilisateur final. StorageCraft ne traite pas de telles données personnelles pour le VAR ni pour l'utilisateur final. En revanche, StorageCraft est responsable du traitement de ces données personnelles et les traite en son nom propre afin de fournir ses produits au VAR et à l'utilisateur final, répondant ainsi à ses obligations envers eux et réalisant ses tâches générales de gestion des relations.
Fournisseur de services gérés (MSP – Vendant des logiciels par abonnement)	Non	Les seules données personnelles que StorageCraft devrait recevoir de la part d'un MSP sont les noms et adresses e-mail des employés du MSP. StorageCraft ne traite pas de telles données personnelles pour le MSP. En revanche, StorageCraft est responsable du traitement de ces données personnelles et les traite en son nom propre afin de fournir ses produits et services au MSP, répondant ainsi à ses obligations envers lui.
Contrat sur les produits cloud	Oui	Un client cloud transfère des sauvegardes à StorageCraft afin que ce dernier les traite en son nom. Comme StorageCraft n'a pas connaissance des types de données présentes dans les sauvegardes, StorageCraft part du principe que ces sauvegardes contiennent des données personnelles. En fournissant ses produits et services cloud, StorageCraft est sous-traitant (et dans certains cas sous-sous-traitant si son client cloud fait appel aux services cloud de StorageCraft pour sauvegarder des données qu'il traite en tant que sous-traitant pour un autre responsable de traitement). Il traite donc les données pour le compte de son client cloud et un ATD est nécessaire.
Contrat de distribution	Non	Un distributeur peut transférer des données personnelles à StorageCraft, associées à des entreprises dans la chaîne de vente, notamment son revendeur ou l'utilisateur final. Ces données personnelles sont généralement composées des noms et adresses e-mail des personnes employées par le distributeur, le revendeur ou l'utilisateur final. StorageCraft ne traite pas de telles données personnelles pour le distributeur ni pour d'autres parties de la chaîne de vente. En revanche, StorageCraft est responsable du traitement de ces données personnelles et les traite en son nom propre afin de fournir ses produits au distributeur, au VAR ou à l'utilisateur final, répondant ainsi à ses obligations envers eux et réalisant ses tâches générales de gestion des relations.

Q. StorageCraft a-t-il désigné un délégué à la protection des données ?

A. Non. On croit souvent à tort que le RGPD nécessite que toutes les entreprises désignent un délégué à la protection des données. Or, ce n'est pas le cas. Le RGPD impose la nomination d'un délégué à la protection des données dans uniquement trois cas très particuliers : (a) le traitement des données est effectué par « une autorité ou un organisme public » ; (b) les « activités principales » du responsable du traitement ou du sous-traitant impliquent la surveillance régulière, systématique et à grande échelle des personnes concernées ; et/ou (c) les « activités principales » du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de données personnelles sensibles. Ces trois cas ne s'appliquent pas à StorageCraft. Même si StorageCraft n'est pas dans l'obligation de nommer un délégué à la protection des données, nous attachons tout de même une très grande importance à la protection des données. La conformité en matière de protection des données est supervisée par nos services juridiques et informatiques.

Q. Quelles sont les mesures de sécurité techniques et organisationnelles adoptées par StorageCraft en lien avec la manière dont elle traite les données personnelles ?

R. Bien que StorageCraft ne puisse pas révéler tous ses processus et toutes ses procédures de sécurité, il s'engage à protéger les données personnelles conformément au RGPD. Un résumé des mesures de sécurité techniques et organisationnelles de StorageCraft est inclus au sein d'un avenant aux ATD de StorageCraft (le cas échéant). Une copie de ces mesures est disponible sur demande.

Q. En quoi consistent les « clauses contractuelles types » ? Par ailleurs, les clauses utilisées par StorageCraft sont-elles conformes au RGPD ?

R. Pour commencer, le RGPD interdit tout transfert de données personnelles en dehors de l'EEE, sauf si ces données personnelles sont protégées de façon adaptée. Les « clauses contractuelles types » (également appelée parfois « clauses modèle ») constituent l'une des méthodes approuvées par la Commission européenne par le biais desquelles les données personnelles peuvent être transférées de manière licite en dehors de l'EEE si elles sont protégées de façon adaptée. Pour pouvoir s'appuyer sur les clauses contractuelles types, celles-ci doivent être reproduites mot pour mot, comme elles figurent dans la décision de 2010 de la Commission européenne qui les a promulguées.personnelles Les clauses contractuelles types de StorageCraft font partie de son ATD et sont conformes aux exigences des lois applicables sur la confidentialité des données, notamment le RGPD.

Q. À quels sous-sous-traitants StorageCraft fait-il appel ?

R. Une liste des sous-sous-traitants de StorageCraft est disponible sur le site Web de StorageCraft.

Q. Si un revendeur à valeur ajoutée achète des produits StorageCraft par l'intermédiaire d'un distributeur, a-t-il besoin du consentement de l'utilisateur final pour fournir au distributeur des données personnelles concernant les employés de l'utilisateur final, notamment le nom et l'adresse e-mail d'un interlocuteur employé par l'utilisateur final ?

R. Nos partenaires doivent mener leur propre analyse de l'effet du RGPD sur leurs pratiques commerciales, et déterminer notamment leurs propres obligations en tant que responsables de traitement de données. Nous leur recommandons de prêter une attention particulière à l'article 6 du RGPD, qui identifie les différentes bases licites pour le traitement des données personnelles, ainsi qu'aux articles 13 et 14, qui identifient les obligations d'un responsable de traitement à informer une personne concernée de l'utilisation de ses données, ce qui est généralement accompli au moyen d'une politique de confidentialité claire et accessible. Les personnes partent souvent du principe que le « consentement » est requis, alors que la seule chose qu'un responsable de traitement peut avoir à faire est de communiquer clairement avec la personne concernée au sujet de l'utilisation et du traitement de ses données personnelles. En vertu de l'article 6, le consentement n'est qu'une des conditions, parmi d'autres, rendant licite le traitement des données personnelles. Un responsable de traitement peut s'appuyer sur le consentement lorsqu'une autre condition rendant le traitement licite existe, mais il n'a pas l'obligation de le faire. La condition rendant le traitement des données licite doit être soigneusement évaluée, car elle a un impact sur les obligations du responsable de traitement à l'égard d'autres dispositions du RGPD, notamment la demande de suppression de données de la part de la personne concernée.

Q. De quelle manière le Brexit affectera-t-il mes données utilisées dans des produits cloud StorageCraft ?

R. Comme les négociations entre le Royaume-Uni et l'Union européenne au sujet du Brexit sont en cours, les effets du Brexit, et notamment son impact sur la protection des données, sont relativement incertains. Bien qu'il soit impossible de se prononcer aujourd'hui au sujet de la loi sur la protection des données du Royaume-Uni post-Brexit, la plupart des indicateurs suggèrent qu'il y aura peu de changements.

Entré en vigueur en mai 2018, le RGPD est actuellement appliqué au Royaume-Uni. Le gouvernement, craignant qu'une trop grande incertitude ait un impact négatif sur les affaires et sur les citoyens, a précisé qu'une grande partie de la législation européenne continuera à s'appliquer au Royaume-Uni après le Brexit. Reste à voir si le Brexit se fera ou non en douceur, mais les autorités chargées de la protection des données au Royaume-Uni ont récemment insisté sur leur engagement en faveur du RGPD. En effet, dans un discours de la commissaire à l'information du Royaume-Uni prononcé en avril 2018, celle-ci a indiqué qu'elle continuait à conseiller le gouvernement et le parlement au sujet d'une « réforme législative garantissant des normes élevées en matière de protection des données aux citoyens et consommateurs britanniques, où que se trouvent leurs données, des flux de données interrompus vers l'Europe et le reste du monde ; et une sécurité juridique pour les entreprises ». Elle a également mis l'accent sur le fait que la protection des données était un « domaine prioritaire » pour l'accord du Brexit et que le bureau du commissaire aux informations (ICO) continuait à jouer un rôle majeur pour créer une orientation pour le RGPD et s'engage toujours auprès du Comité européen de la protection des données (CEPD) (anciennement groupe de travail Article 29). Elle a également précisé que la Première ministre Theresa May avait récemment plaidé en faveur d'un rôle continu de l'ICO sous la forme d'un siège au sein de la CEPD, avec un droit de vote ou une relation substantielle de ce type.

Après le Brexit, les entreprises vendant des produits et des services au Royaume-Uni devront être conformes au RGPD, mais aussi à l'équivalent britannique du RGPD. Nous nous attendons toutefois à un chevauchement important (voire total) entre ces deux législations. Comme le RGPD est déjà en vigueur au Royaume-Uni, même si le Brexit se révélait être plutôt un « Brexit dur » qu'un « Brexit mou », nous estimons que le Royaume-Uni devrait être un pays apte à recevoir des données de l'EEE, et vice versa.

Par conséquent, nous ne voyons pas la nécessité de déplacer des données de nos centres de données StorageCraft de Dublin ou de Francfort, ni de modifier les politiques de nos produits pour le moment. Cela étant, StorageCraft a conscience de la nécessité qu'il y a à garantir la conformité avec le RGPD et la loi britannique sur la protection des données post-Brexit. À l'approche du Brexit, nous examinerons quel effet (le cas échéant) ce dernier peut avoir sur nos produits et services primés. Nous vous ferons alors part de nos conclusions.

Q. De quelle manière le « droit à la suppression des données » affecte-t-il les données contenues dans les sauvegardes ?

R. Le droit à la suppression des données, appelé également « droit à être oublié », est l'un des droits accordés aux personnes concernées par les données. Dans certains cas, celui-ci permet à une personne concernée de demander au responsable de traitement d'effacer des données lui appartenant.

Comme avec toute législation, certains problèmes ne sont pas spécifiquement abordés par le RGPD. C'est notamment le cas de l'interaction entre le droit à la suppression et les copies de sauvegarde. Avec une copie de sauvegarde, il peut être impossible d'isoler des données personnelles d'une personne concernée et de les supprimer, tout en maintenant l'intégrité de la sauvegarde. Par ailleurs, même dans les cas où cela est possible, les coûts associés à un tel effort peuvent être totalement irréalistes. Ce problème nécessite des clarifications ou des orientations de la part du CEPD, en particulier du fait que le RGPD indique lui même que la capacité à restaurer des données personnelles depuis une copie de sauvegarde est l'une des « mesures organisationnelles et techniques appropriées » qui doivent être mises en œuvre pour garantir la sécurité des données. (Voir art. 32(1)c.)

Bien qu'aucune réponse claire n'ait été donnée pour l'instant, l'ICO du Royaume-Uni est l'une des rares autorités nationales de protection des données à s'être intéressée au problème. Avant le RGPD, l'ICO a publié un document d'orientation intitulé « Deleting personal data » (Suppression des données personnelles). Ce document a reconnu la difficulté que présente une demande de suppression de données en cas de données archivées ou sauvegardées. Le document indique que « l'ICO adoptera une approche réaliste pour reconnaître le fait que la suppression d'informations d'un système n'est pas toujours un processus simple et qu'il est possible de mettre des informations 'hors d'usage' et que les questions de conformité en matière de protection des données soient

« suspendues » à condition que certaines mesures de sécurité soient mises en place. » Pour l'ICO, les données personnelles faisant l'objet d'une demande de suppression peuvent être mises « hors d'usage » au lieu d'être réellement supprimées, si le responsable de traitement :

- ne peut pas utiliser ou n'utilisera pas les données d'une manière qui affecte la personne concernée ;
- ne permet pas à une autre organisation d'accéder aux données ;
- applique des « mesures de sécurité techniques et organisationnelles adaptées » aux données ; et
- s'engage à supprimer les données si ou quand la suppression devient possible.

L'ICO a cité à plusieurs reprises cette orientation pré-RGPD, en indiquant qu'elle serait mise à jour « en temps voulu ». Après la mise en place du RGPD, l'ICO a continué à se reposer sur cette orientation en soulignant le fait que, lorsqu'il s'agit de supprimer des données contenues dans une copie de sauvegarde, mettre ces données « hors d'usage » de la manière décrite ci-dessus est une approche acceptable pour répondre aux demandes de suppression de données impliquant des données de sauvegarde. L'ICO ajoute qu'un responsable de traitement « doit être parfaitement clair avec les personnes concernées au sujet du devenir de leurs données une fois la demande de suppression traitée, notamment en ce qui concerne les systèmes de sauvegarde ». StorageCraft recommande d'informer la personne concernée que ses données personnelles contenues dans la sauvegarde n'ont pas été supprimées, mais mises « hors d'usage » par l'application des conditions précédentes. En l'attente d'une clarification du RGPD, que ce soit de manière législative ou par le biais d'orientations de la part du CEPD, StorageCraft estime que la solution précédente est la meilleure solution à ce dilemme.

Q. Où puis-je trouver plus d'informations concernant l'approche de StorageCraft en matière de confidentialité des données ?

R. Peu de temps après l'entrée en vigueur du RGPD, StorageCraft a publié une mise à jour de sa politique de confidentialité, disponible sur le site Web de StorageCraft. Ce document fait office de point de départ pour toute question concernant les données personnelles collectées par StorageCraft et la manière dont elle les utilise. Pour toute autre question ou préoccupation en matière de confidentialité, vous pouvez nous contacter à l'adresse privacy@storagecraft.com (en anglais).

CETTE FAQ A ÉTÉ ÉLABORÉE PAR STORAGECRAFT TECHNOLOGY ET REFLÈTE L'OPINION DE LA SOCIÉTÉ CONCERNANT LE SUJET ABORDÉ. ELLE NE CONSTITUE PAS UN AVIS JURIDIQUE. DEMANDEZ L'AVIS DE VOTRE PROPRE CONSEILLER JURIDIQUE CONCERNANT LA QUESTION SOULEVÉE DANS LE PRÉSENT DOCUMENT.

StorageCraft.