sage

RGPD

LE GUIDE POUR LES PETITES ET MOYENNES ENTREPRISES

Les informations dont vous avez besoin pour comprendre et aller de l'avant

#IProtectData

Partagez le message. Partagez la responsabilité.

TABLE DES MATIÈRES

INTRODUCTION

Le règlement général sur la protection des données (RGPD) a été décrit comme le plus gros remue-ménage concernant la manière dont les données à caractère personnel sont recueillies, stockées et utilisées.

Ses implications sont énormes certainement non entièrement comprises par de nombreuses entreprises, en dépit du fait que la législation sera en vigueur dès le 25 mai 2018.

Le RGPD porte bien au-delà de la législation existante sur la protection des données, telle que la loi informatique et liberté de 1978 en France, et affecte les entreprises de toutes tailles, des entreprises individuelles aux plus grands groupes. Les recherches entreprises par Sage* révèlent que 60 % des entreprises françaises manquent d'informations sur le RGPD et que 57 % ne comprennent pas ce que le RGPD signifie pour leur entreprise.

Celui-ci affectera pourtant votre manière de gérer votre activité, notamment en termes de marketing, et également la manière dont vous traitez les informations telles que les données sur votre personnel et les données internes se rapportant à l'exploitation de votre entreprise.

Avec la perspective d'amendes allant jusqu'à 4 % du chiffre d'affaires global annuel ou 20 millions d'euros, le chiffre le plus élevé prévalant, il est important de comprendre le RGPD et ses impacts sur votre activité. Notamment, il est possible que vous soyez sanctionné pour une violation du règlement même en l'absence de perte de données réelle.

Ce guide concis est destiné aux petites et moyennes entreprises afin de les aider à se préparer à la mise en vigueur du RGPD, mais ne peut remplacer un audit complet effectué par un professionnel dûment qualifié. Veuillez prendre connaissance des mentions légales de Sage à la page 05 ci-après.

*Enquête concernant le RGPD menée par Sage auprès de ses clients par Sage, octobre 2017

> Il s'agit simplement d'une nouvelle législation. Vous pouvez mettre en place un plan, appliquer quelques nouvelles mesures et poursuivre vos activités quotidiennes. Il n'y a aucune raison de céder à la panique. Cependant, vous ne pouvez pas ignorer le RGPD.

Orlagh Kelly

Avocate et PDG de Briefed, spécialistes en conformité et formation RGPD

COMMENT LIRE CE GUIDE

Ce guide contient différentes sections, vous pouvez choisir de commencer la lecture à partir de la section de votre choix.

Pour un examen approfondi du RGPD, voir la page **07**

Cliquez ici pour consulter

Pour savoir quelle pourrait-être la prochaine étape à suivre, voir la page **15**

Cliquez ici pour consulter

Pour les réponses à des questions types posées par des entreprises au sujet du RGPD, voir **25**

Cliquez ici pour consulter

LIMITATION DE RESPONSABILITÉ SAGE

Les informations communiquées dans ce guide sont fournies à titre indicatif uniquement. Elles ne visent pas à constituer un conseil juridique et ne doivent pas être interprétées comme tel. Nous tenons à souligner que, pour les clients qui ne sont pas certains des implications du RGPD pour leurs activités, rien ne peut remplacer la conduite de leur propre enquête approfondie ou l'obtention de conseils juridiques spécifiques à leur situation.

Bien que nous ayons tout mis en œuvre pour faire en sorte que les informations apportées sur ce site Internet soient exactes et actualisées, Sage ne fait aucune promesse quant à leur exhaustivité ou à leur exactitude, et les informations sont fournies « telles quelles » sans aucune garantie, expresse ou implicite. Sage ne pourra être tenu responsable d'éventuelles erreurs ou omissions et sa responsabilité ne saurait être engagée pour tout dommage (y compris, mais sans s'y limiter, les pertes commerciales ou les pertes de bénéfices), contractuel, délictuel ou autre, résultant de l'utilisation de ces informations ou de la confiance accordée à ces informations, ou de toute mesure ou décision prise à la suite de l'utilisation de ces informations.

PRINCIPALES CARACTÉRISTIQUES DU RGPD

Droits des personnes

Développe considérablement les droits des personnes et le nombre d'informations à leur communiquer au sujet du traitement.

Consentement

Doit être confirmé par une déclaration ou un acte positif clair. Le consentement ne peut être tacite et les cases précochées sur les sites web sont interdites.

Délégué à la protection des données

Peut être obligatoire dans certains cas. A une connaissance approfondie de la loi sur la protection des données. Salarié ou employé sous contrat de prestation de services.

Sanctions

Jusqu'à 4 % du CA annuel mondial ou 20 millions d'euros (le montant le plus élevé étant retenu). Une amende est possible même sans perte de données.

Respect de la vie privée tout au long du processus

Le traitement intègre la vie privée à chaque étape et n'utilise que les données strictement nécessaires à la finalité indiquée.

Portabilité des données

Les personnes peuvent récupérer, stocker ou transmettre leurs données, même chez un concurrent.

Champ d'application élargi

S'applique à votre entreprise et à celles traitant les données pour vous, même en dehors de l'UE.

Notification obligatoire des failles de sécurité

Les responsables de traitement des données en France doivent prévenir l'Autorité de contrôle compétente 72 heures maximum après en avoir pris connaissance. Doivent avertir la personne concernée en cas de risque élevé pour les droits et libertés de la personne concernée.

Source : Règlement général sur la protection des données (RGPD) : Le guide pratique Sage pour les entreprises

LE RGPD EN DÉTAIL

Voici une introduction concise des concepts et termes essentiels dans le cadre du RGPD.

La terminologie

De façon quelque peu surprenante, maîtriser le RGPD ne réclame pas nécessairement une compréhension du jargon juridique ni d'une terminologie complexe. Toutefois, il y a quelques exceptions se rapportant à des termes qu'il est bon de connaître le plus tôt possible étant donné que vous devrez les utiliser dans votre documentation de conformité au RGPD.

Le RGPD identifie les rôles clairs qui déterminent les paramètres pour la façon dont les données à caractère personnel sont traitées et, par conséquent, ce qu'on exige de vous. En tant qu'entreprise, vous devez savoir à quelle catégorie parmi les suivantes vous appartenez :

Responsable de traitement des données : La personne, l'autorité publique, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel. Si vous recueillez des données à caractère personnel pour votre propre usage et à des fins personnelles, vous êtes le responsable de traitement des données et entièrement responsable de la conformité au RGPD, y compris la sécurité dans son ensemble.

Responsable de traitement : Une personne, autorité publique, agence ou tout autre organisme qui traite les données à caractère personnel pour le compte responsable de traitement des données. Si vous traitez des données à caractère personnel pour le compte d'une autre organisation, vous êtes le processeur de données et devez agir uniquement selon les instructions de l'organisation de contrôle. Toutefois, vous êtes également responsable de toute obligation de conformité au RGPD imposée sur les processeurs de données.

Co-responsables de traitement des données ou responsables de traitement des données en commun : Il peut y avoir parfois des co-responsables de traitement des données, cas de figure dans lequel deux ou plus de responsables décident ensemble de la raison pour laquelle les données à caractère personnel sont recueillies et utilisées. Par exemple, un fabricant peut partager des données clients avec ses détaillants, car ils y ont un intérêt commun. Il peut également y avoir des responsables de traitement des données en commun, cas de figure dans lequel où deux ou plus de responsables partagent les mêmes données, mais les traitent indépendamment les uns des autres. Un comptable peut être un responsable de traitement en commun avec vous, car il doit traiter les données de vos clients dans le cadre du processus de comptabilité, par exemple.

Dans cet exemple, Bertrand Frères est le responsable de traitement des données tandis que Dupond SARL est un processeur de données.

Une des nouveautés du RGPD consiste en ce que les responsables de traitement des données et les processeurs de données sont responsables de toute violation affectant les données à caractère personnel. Toutefois, les responsables de traitement des données doivent veiller à ce que les responsables de traitement fournissent des « garanties suffisantes » de conformité au RGPD, et à ce que les droits en matière de données personnelles soient protégés.

Le sujet des données : Il s'agit de la manière dont le RGPD désigne une personne naturelle identifiée ou identifiable à laquelle on peut se référer par référence à ce qui est considéré en tant que données à caractère personnel (voir ci-dessous).

Les données à caractère personnel : Ceci inclut, sans s'y limiter : un nom, un numéro d'identification, des données de localisation, ou un identifiant en ligne, ou un ou plusieurs facteurs spécifiques se rapportant à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de l'individu concerné.

Les catégories spéciales de données : Il s'agit de données révélant l'origine ethnique ou raciale, les opinions politiques, les croyances religieuses ou philosophiques, ou l'appartenance à un syndicat, et le traitement de données génétiques, de données biométriques visant à identifier de manière unique une personne, de données concernant la santé ou de données concernant la vie ou l'orientation sexuelle, et celles-ci nécessitent une plus grande protection.

Pour finir, il est important de clarifier ce qu'on entend par traitement de données :

Le traitement : Toute opération ou tout ensemble d'opérations exécutées sur des données à caractère personnel, y compris par des moyens automatisés, tels que la collection, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, la récupération, la consultation, l'utilisation, la divulgation par transmission, diffusion ou toute autre forme de mise à disposition, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction.

Les termes ci-dessus sont utilisés dans ce guide.

Les préceptes de base de la protection des données de base

Le RGPD se base sur les principes existants de protection des données avec lesquels, en tant qu'entreprise, vous devriez être familiarisé. Ceux-ci sont résumés comme suit :

Les principes de la protection des données

Les données à caractère personnel doivent être traitées licitement, de façon équitable et d'une manière transparente par rapport à l'individu concerné. Elles doivent être recueillies à des fins spécifiées, explicites et légitimes et ne doivent pas être autrement traitées d'une manière incompatible avec lesdites dispositions.

Les données à caractère personnel recueillies doivent être adéquates, pertinentes et limitées à ce qui est nécessaire. Elles doivent être exactes et mises à jour, et toutes les mesures raisonnables doivent être prises pour veiller à ce que les données à caractère personnel qui sont inexactes soient effacées ou rectifiées sans délai. Elles doivent être stockées d'une manière qui identifie l'individu uniquement pour la durée nécessaire, et elles doivent être traitées d'une manière assurant une sécurité appropriée, y compris la protection contre la perte, la destruction, ou l'endommagement, et l'accès non autorisé et illicite.

La licéité du traitement

Le traitement des données à caractère personnel est uniquement licite si au moins l'une des conditions suivantes est remplie :

1. La personne a accordé son consentement pour une ou plusieurs finalités spécifiques ;
2. Le traitement est nécessaire pour exécuter un contrat dont la personne concernée est ou sera bientôt partie prenante ;
3. Le traitement est nécessaire pour se conformer à une obligation légale (par ex. la soumission de dossiers fiscaux par une entreprise) ;
4. Il existe une mission d'intérêt public ou qui est effectuée dans l'intérêt de l'autorité publique ;
5. Le traitement est nécessaire afin de protéger les intérêts vitaux du sujet des données ou d'une autre personne naturelle (situations de vie ou de mort) ;
6. Le traitement est nécessaire aux fins des intérêts légitimes du responsable de traitement (ou d'un tiers), à moins que ne prévalent les intérêts, les droits fondamentaux ou les libertés de la personne concernée.

Les transferts internationaux

Le RGPD prolonge l'interdiction générale de transférer des données à caractère personnel en dehors de l'Espace économique européen vers un pays n'offrant pas un niveau de protection adéquat pour lesdites données. Au moment de la rédaction de ce document, les pays reconnus par la Commission européenne comme offrant une protection « adéquate » sont : les entreprises américaines qui ont certifié respecter l'accord Privacy Shield Union européenne-États-Unis (remarque : ce n'est pas pour autant que les États-Unis sont reconnus comme un pays offrant une protection adéquate), Andorre, l'Argentine, le Canada (limité à la loi canadienne relative à la confidentialité des données, connue sous le nom PIPEDA), les îles Féroé, Guernesey, Israël, l'île de Man, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay. En l'absence de décision d'adéquation, les transferts ne peuvent avoir lieu que dans des circonstances limitées, notamment, sur la base du consentement, l'utilisation des clauses contractuelles types publiées par la Commission européenne ou, dans le cas des transferts inter-sociétés, l'utilisation des Règles d'entreprise contraignantes (BCR, Binding Corporate Rules).

Les principes du RGPD

Le RGPD s'appuie sur les principes de base suivants et a pour objectif de fournir une norme minimum pour la protection des données.

Élargissement du champ et de la zone géographique

Précédemment, seules les autorités de contrôle étaient directement responsables des violations affectant les données à caractère personnel. En vertu du RGPD, les responsables de traitement des données et les processeurs de données sont désormais responsables.

De plus, ce ne sont pas seulement les responsables de traitement des données et les processeurs de données dans l'UE qui sont affectés, mais également ceux hors de l'UE qui offrent des biens ou des services aux individus de l'UE, indépendamment de toute exigence de paiement ; ou qui contrôlent le comportement d'individus dans l'UE.

Il se peut que ces sociétés doivent désigner un représentant de l'UE pour se conformer au RGPD en leur nom si leur traitement de données à caractère personnel est fréquent, ou inclut le traitement à grande échelle de catégories spéciales de données, ou implique le traitement de données se rapportant à des catégories spéciales de données.

La comptabilité et la tenue des registres

En vertu du RGPD, les responsables de traitement des données doivent être en mesure de prouver qu'elles sont conformes. Ceci est partiellement accompli en se conformant à certaines exigences de registres plutôt onéreuses. En particulier, les registres tenus doivent détailler les points suivants :

1. activités de traitement (en cas d'emploi de plus de 250 personnes, ou moins si le traitement représente un risque en matière de droits et de libertés des personnes, n'est pas occasionnel, ou inclut des catégories spéciales de données) ;
2. demandes d'accès au sujet ;
3. violations ;
4. manière dont les consentements sont obtenus ; et
5. évaluations de l'impact sur la vie privée (voir ci-dessous).

Il est également exigé des processeurs de données de tenir des registres de leurs activités de traitement bien que les exigences ne soient pas aussi détaillées que celles des responsables de traitement des données.

Le respect de la vie privée dès la conception et par défaut

Le RGPD introduit deux nouveaux concepts majeurs.

Le "Privacy by Design" est un concept qui impose aux entreprises d'intégrer les principes du RGPD dès la conception d'un projet, d'un service ou de tout autre outil lié à la manipulation de données personnelles. Le suivi peut être assuré par une formation continue, la mise en place d'audits réguliers, la restriction de l'accès aux données à caractère personnel selon le principe du besoin d'en connaître et la mise en œuvre de mesures de sécurité techniques et organisationnelles appropriées telles que la pseudonymisation et le cryptage.

Le RGPD réclame également la conduite d'évaluations de l'impact sur la vie privée en cas de risque élevé pour les données à caractère personnel. Il s'agit d'un procédé systématique, généralement un questionnaire, pour l'évaluation des effets potentiels sur la vie privée des individus d'un projet, d'une initiative ou d'un système ou plan proposé.

Le respect de la vie privée par défaut exige que vous mettiez en œuvre des mesures de sécurité techniques et opérationnelles appropriées pour s'assurer, par défaut, que seules les données à caractère personnel nécessaires au traitement soient effectivement traitées (un procédé dénommé intitulé « minimisation des données »).

Le signalement obligatoire des violations

Les responsables de traitement doivent notifier les autorités de contrôle telles que la CNIL en France dans les 72 heures après en avoir été informées. Si la faille présente un risque élevé pour les individus concernés, les responsables de traitement des données doivent en être informés dans les plus brefs délais. Les processeurs de données doivent informer les responsables de traitement des données de toute violation dans les plus brefs délais.

L'obtention du consentement auprès de clients

Comme susmentionné, (voir Licéité du traitement en à la page 9), le consentement est un des moyens de s'assurer que les données à caractère personnel sont traitées en toute licéité. Par exemple, si vous êtes déjà engagé dans un contrat avec un individu, ou si vous le serez bientôt, le consentement n'est pas exigé.

Toutefois, et comme auparavant, lorsque le consentement est exigé, celui-ci doit être accordé librement, de manière spécifique, informée et dépourvue de toute ambiguïté.

En vertu du RGPD, le consentement doit également être confirmé par une déclaration ou toute autre action affirmative claire. Ceci signifie que le silence, les cases pré-cochées sur les pages Web et l'inactivité ne constituent plus un consentement. Répondre « oui » au téléphone peut être considéré comme un consentement, mais des enregistrements doivent être conservés.

Étant donné que le consentement doit désormais être spécifique, le RGPD énonce clairement qu'il ne peut pas faire partie d'une « offre groupée ».

En d'autres termes, des consentements séparés sont nécessaires pour différentes opérations de traitement de données.

Pour finir, les personnes doivent être informées qu'elles ont le droit de retirer leur consentement à tout moment et que le retrait de leur consentement doit être aussi facile que la procédure d'obtention de consentement.

Les droits de vos clients

Vos clients (c.-à-d. les sujets des données) sont habilités à recevoir des informations sur la manière dont vous utilisez leurs données à caractère personnel. De fait, le RGPD réclame que les responsables de traitement des données fournissent même davantage d'informations que ce qui était précédemment exigé. Les informations relatives à ces droits sont généralement délivrées sous la forme d'un « avis de confidentialité », souvent sur un site Web, mais la procédure entière se doit d'être transparente.

En particulier, les personnes doivent être informées qu'elles ont les droits (non exhaustifs) suivants :

1. se plaindre aux autorités de contrôle, telles que la CNIL en France ;
2. retirer leur consentement au traitement de leurs données personnelles (voir ci-dessous) ;
3. accéder à leurs données personnelles et les faire rectifier ou effacer (processus également connu sous le nom de « droit à l'oubli ») ;
4. être informés de l'existence de tout traitement automatisé de données à caractère personnel (y compris le profilage) ;
5. s'opposer à certains types de traitement, par exemple le marketing direct et les décisions basées uniquement sur le traitement automatisé ;
6. être informés de la durée pendant laquelle leurs données personnelles seront conservées ;
7. et obtenir des détails de tout délégué à la protection des données désigné.

Les individus ont également le droit à la « portabilité des données », c'est-à-dire que les données à caractère personnel automatisées qui ont été fournies au responsable de traitement par le sujet des données en vertu d'un consentement ou d'un contrat leur soient retournées ou envoyées directement à un autre responsable de traitement des données. Il se peut même qu'il s'agisse de l'un de vos concurrents, mais ne croyez pas que vous pouvez leur compliquer la tâche, les données à caractère personnel doivent être envoyées dans un format structuré, couramment utilisé et lisible par machine, de manière à ce qu'il soit possible de déplacer, copier ou transférer les données à caractère personnel d'un environnement informatique à l'autre.

Le délégué à la protection des données

En vertu du RGPD, les responsables de traitement des données doivent désigner un délégué à la protection des données (DPO) auprès duquel :

(1) le traitement est effectué par une autorité publique ou un organisme public, excepté les tribunaux dans l'exercice de leurs fonctions juridictionnelles ;

(2) les activités principales du responsable de traitement des données ou du processeur de données consistent en des opérations de traitement qui, en vertu de leur nature, de leur champ d'application et/ou de leurs finalités, nécessitent un suivi régulier et systématique à grande échelle ;

(3) les activités principales du responsable de traitement des données ou du processeur de données consistent en un traitement à grande échelle de catégories spéciales de données et de données à caractère personnel se rapportant à des condamnations pénales et des actes criminels.

Votre DPO peut être un employé ou vous pouvez faire appel à utiliser un tiers, mais vous devez informer la CNIL de l'identité de votre DPO.

Le DPO aura pour rôle d'informer la société et son personnel de leurs obligations en vertu du RGPD. Le DPO devra également assurer le suivi de la conformité avec le RGPD (et toute autre loi ou exigence sur la protection des données). Ceci pourrait inclure la gestion des évaluations d'impact sur la protection des données, la conduite d'audits internes et l'organisation de la formation du personnel. Le DPO sera également le premier point de contact pour les investigations relatives à la protection des données menées par les autorités de contrôle (comme la CNIL en France), et le point de contact pour tout individu dont les données sont traitées par la société, y compris les clients et les employés.

« La meilleure façon de démarrer ce projet est d'obtenir les services d'un expert pour effectuer une analyse des lacunes, car ceci permet de faire ressortir tous les problèmes, de les cerner clairement, de les organiser de façon méthodique puis de les rectifier. »

Je pense que de nombreuses sociétés sont surprises par le niveau de détails du RGPD et l'ampleur de son champ d'application dans toute l'entreprise et les différents services concernés.

Une perception erronée serait de penser qu'il s'agit d'une tâche qui revient au service informatique, ce qui n'est absolument pas le cas. De fait, l'entreprise dans son ensemble doit être impliquée. Chaque personne doit être formée pour comprendre ce qu'elle peut ou ne peut pas faire.

Orlagh Kelly

Avocate et PDG de Briefed, spécialistes en conformité et formation RGPD

Les amendes et responsabilités

Comme susmentionné, en cas de non-respect du RGPD, les amendes peuvent atteindre jusqu'à 4 % du chiffre d'affaires global annuel ou 20 millions d'euros, le chiffre le plus élevé étant retenu. Ceci s'applique aussi bien aux responsables de traitement des données qu'aux processeurs de données.

Les autorités de contrôle telles que la Commission Nationale de l'Informatique et des Libertés (CNIL) en France seront chargées d'enquêter sur les violations de données ou autres transgressions du RGPD et pourront potentiellement infliger des amendes. La CNIL déclare que toutes les amendes sont transmises directement au gouvernement.

ÊTES-VOUS CONFORME AVEC LE RGPD ?

En vertu du RGPD, il existe six bases légales pour la manipulation et le traitement des données à caractère personnel des individus, comme suit. Au moins une condition doit être remplie.

Les intérêts légitimes	Ceci est un domaine subjectif et les entreprises doivent trouver un équilibre entre le droit à utiliser les données d'un individu et le droit de l'individu à refuser l'utilisation de ses données. Les entreprises doivent clairement et incontestablement justifier la raison pour laquelle les données d'un individu doivent être utilisées et la bonne pratique est de documenter le raisonnement qui sous-tend votre décision.
Le consentement	Le consentement doit être accordé librement, de manière informée et dépourvue de toute ambiguïté, et peut être obtenu dans plusieurs formats (par ex. en ligne via une case à cocher), ou en répondant « oui » dans le cadre d'un appel téléphonique, mais un enregistrement de ce consentement doit alors être conservé.
Le contrat	Ceci se rapporte au traitement nécessaire de données à caractère personnel dans le cadre d'un contrat auquel le sujet des données est partie prenante, ou afin de prendre des mesures à la demande du sujet des données avant la passation d'un contrat, et reste inchangé en fonction des réglementations actuelles sur la protection des données.
L'obligation juridique	Des exemples d'obligations juridiques incluent celles qui entrent dans le cadre d'une conformité fiscale avec l'Administration fiscale ou des finalités de prévention des fraudes en vertu des réglementations financières.
Les intérêts vitaux	Le traitement des données à caractère personnel est autorisé par une organisation afin de protéger les intérêts vitaux du sujet des données. En substance, ceci se rapporte aux questions « de vie ou de mort ».
L'intérêt public	Applicable dans le cas où des données à caractère personnel doivent être traitées dans l'intérêt public, par exemple, se rapportant à la performance des tâches accomplies par une autorité publique.

PRÉPARATION AU RGPD

Voici quelques mesures que vous pouvez envisager. N'oubliez pas que les mesures de préparation au RGPD prennent généralement deux formes : traitement des questions internes, comme s'assurer de la conformité de la manière dont vous traitez les données des employés, et traitement des questions externes, comme s'assurer de la conformité de la manière dont vous gérez les données des clients. Ces deux formes doivent être prises en considération avec la même importance.

Les choses à faire dès maintenant

Voici certaines choses que vous pouvez décider de faire le plus tôt possible.

Informez votre personnel et vos fournisseurs

Il est peu probable que les effets du RGPD épargnent totalement certains membres du personnel d'une entreprise, qu'il s'agisse de la manière dont ils remplissent leurs fonctions ou de la manière dont l'entreprise va les gérer une fois le RGPD mis en place. Vous devez commencer par les informer des changements probables à venir. Vous pouvez réclamer à votre personnel d'effectuer ses propres recherches pour voir comment leur rôle de chacun va être affecté, surtout si les employés en question appartiennent à un syndicat ou à un organisme professionnel qui pourrait être en mesure de les informer en matière de RGPD.

Toute société ou agence tierce que vous utilisez devra également être conforme au RGPD. Il vous faut donc entamer des discussions avec celles-ci.

Identifiez

Adoptez l'approche du « quoi, quand, où, pourquoi et comment ». Il est probable que toutes les fonctions au sein d'une entreprise vont être affectées par les exigences du RGPD en matière de licéité du traitement des données. Vous devriez établir une liste des domaines de votre entreprise qui nécessitent votre attention et votre focalisation, puis tentez de créer un calendrier des changements à mettre en place.

En fonction de la structure de votre entreprise, vous pouvez choisir de contacter les chefs de service et de leur demander de créer des plans de mise en œuvre du RGPD.

Réexaminez les données existantes que vous détenez

Examinez les données dans chacune des fonctions de votre entreprise. N'oubliez pas que les données peuvent prendre toutes sortes de formes. Bien que les bases de données client puissent constituer une cible évidente pour un examen, les e-mails et les SMS peuvent relever du champ d'application du RGPD.

Consultez votre liste de clients. Disposez-vous d'une base juridique pour le traitement des données à caractère personnel de chaque individu inclus dans la liste (voir la page 14 pour plus d'informations) ? Si tel n'est pas le cas, quels plans pouvez-vous mettre en place pour disposer de la base juridique ?

Recherches

Il existe un large ensemble d'informations relatives au RGPD, mais veillez aussi à consulter les informations fournies par les autorités de contrôle.

Vous pouvez trouver d'autres personnes évoluant dans le même secteur que vous qui partagent en ligne leur expérience en matière de mise en œuvre du RGPD. Ceci peut s'avérer un raccourci utile pour obtenir des informations cruciales.

Aller de l'avant

Voici quelques tâches et objectifs pour la mise en œuvre des mesures après votre examen immédiat des exigences du RGPD.

Organisez un audit de RGPD

Il est possible que vous décidiez de vérifier vous-même la conformité de votre entreprise avec le RGPD, mais le caractère spécifique du travail, ainsi que le temps que cette tâche implique, sera peut-être mieux géré par une personne dûment qualifiée qui produira un rapport détaillant les mesures requises.

Il existe différents types de services de consultants en RGPD et, en fonction de la nature et de la taille de votre entreprise, il se peut que vous deviez consulter plus d'un prestataire.

Certaines entreprises offrant un audit RGPD complet se concentrent sur l'informatique et, bien que ceci constitue un élément important du processus, le RGPD réclamera la formation du personnel et, potentiellement, un changement culturel majeur au sein de votre entreprise en matière de relations avec vos clients. Par conséquent, vous devez veiller à trouver un ou des auditeurs qui répondent à vos besoins. Voir page 13.

Désignez d'un délégué à la protection des données

Si votre entreprise exige un délégué à la protection des données (DPO) (voir la page 11), vous devez en désigner un. Il peut s'agir d'un membre de votre effectif existant, d'un nouveau membre de l'effectif ou d'une personne d'une agence externe. Toutefois, vous devrez signaler à la CNIL de qui il s'agit.

Communiquez des informations sur le respect de la vie privée

Réexaminez vos avis de confidentialité et mettez en place des programmes pour effectuer les changements nécessaires en temps voulu. Le RGPD inclut des exigences supplémentaires pour la délivrance d'informations aux clients lors du traitement de leurs données (voir Droits de vos clients en à la page 11).

Établissez des procédures de réponse au RGPD

Le RGPD introduit une exigence juridique stipulant que les responsables de traitement des données doivent signaler toute violation dans les 72 heures après en avoir été informé. Par conséquent, il vous faudra mettre à disposition les ressources nécessaires pour permettre aux employés de se plier à cette exigence, ainsi que des ressources pour veiller au suivi continu de ce processus. Si vous employez un DPO, ceci entre dans ses compétences.

Comme les individus sont habilités par le RGPD à entreprendre des actions telles que le retrait de leur consentement pour le traitement de leurs données à caractère personnel, ou à accéder à leurs données et les effacer ou les transférer, et plus encore, vous devez vous assurer d'avoir toujours les moyens de répondre à ces requêtes. Là encore, un DPO s'occupera de cela si votre entreprise en exige un.

Le réexamen et le suivi

Contrairement à la législation sur la protection des données, la mise en œuvre du RGPD n'est pas un processus ponctuel. Le RGPD impose certaines règles aux entreprises pour s'assurer qu'elles mettent en place un respect de la vie privée dès la conception et par défaut. Ceci signifie que tous les nouveaux procédés, systèmes et plus encore, devront être créés en fonction des exigences du RGPD.

Tout processeur de données tiers que vous engagez dans votre entreprise doit faire l'objet d'une évaluation en termes de conformité au RGPD, car le RGPD stipule que la responsabilité en la matière vous incombe. Vous pouvez donc, par exemple, décider de mettre en œuvre des audits périodiques desdits tiers.

Comprenez vos responsabilités à l'international

Si votre entreprise opère dans plus d'un état membre de l'UE, vous devez déterminer qui est votre principale autorité de contrôle de protection des données et produire des documents à cet effet.

EXEMPLES DU RGPD DANS LA PRATIQUE

Le RGPD s'appuie sur les principes de base suivants et a pour objectif de fournir une norme assurant la protection des données.

Les ventes et le marketing

Les nouvelles exigences du RGPD sont plus strictes en matière de consentement et peuvent impacter les processus de marketing et de gestion de la clientèle de manière particulièrement dure.

Voici quelques exemples généraux de la manière dont le RGPD va affecter une petite entreprise en tenant compte des réserves suivantes. En premier lieu, il ne s'agit pas d'une liste exhaustive et ceci ne constitue pas non plus une alternative à des conseils juridiques éclairés ni à l'examen détaillé de vos propres procédures et méthodes (voir les Mentions légales en à la page 5).

En second lieu, au moment de la rédaction, l'impact exact du RGPD n'est pas encore connu. Par exemple, nous manquons d'exemples pratiques de ce que les autorités de contrôle, telles que la CNIL en France, vont juger acceptable ou non, et une certaine partie de la formulation du RGPD est ouverte à l'interprétation. Par conséquent, ce qui est détaillé ici ne peut être considéré, au mieux, que comme une supposition éclairée.

Les données de marketing existantes

En termes simples, avec les bases de données existantes pour les prospects ou leads de marketing, vous devrez accomplir deux tâches, au moins, avant la mise en œuvre du RGPD :

1. Réexaminer du point de vue juridique le consentement qui a été utilisé à l'origine et déterminer s'il est compatible aux exigences du RGPD (voir Droits de vos clients en page 11) ;
2. Dans le cas vraisemblable probable où votre consentement existant n'est pas suffisant, et qu'il n'y a aucun autre fondement pour le traitement licite des données (voir Licéité du traitement en à la page 9), vous devrez contacter chacun des individus dans votre la base de données pour obtenir un nouveau consentement. Si vous ne recevez pas de consentement nouveau et spécifique concernant les manières dont vous souhaiteriez traiter les données, les données de l'individu concerné devront être supprimées ou effacées.

Il a été estimé que les exigences ci-dessus pourraient signifier se traduire par une réduction des bases de données telles que celles pour la vente et le marketing allant jusqu'à 75 %. Toutefois, il a également été souligné que les clients qui accordent un nouveau consentement se révèlent d'autant plus précieux car cela témoigne de leur volonté à s'engager auprès de votre entreprise.

N'oubliez pas que le consentement n'est qu'une exigence possible pour le traitement licite des données (voir Licéité du traitement en page 9). Si un contrat entre vous et un client existe déjà, où est en passe d'être signé, il n'est pas nécessaire d'obtenir un consentement, par exemple, lorsque le traitement est nécessaire pour l'exécution d'un contrat ou dans l'intérêt légitime de votre entreprise et/ou du client.

Le consentement pour aller de l'avant

Bien évidemment, vous devrez créer de nouvelles procédures compatibles avec le RGPD pour toute donnée à caractère personnelle que vous recueillez auprès d'individus à partir du 25 mai 2018 et ceci peut impliquer l'obtention d'un consentement.

Rappelez-vous que vous ne pouvez plus présumer du consentement d'un individu dans le cadre d'un projet, d'un service ou de tout autre outil lié à la manipulation de données personnelles (voir Obtention du consentement auprès des clients en page 11).

Avant d'acquérir un prospect ou lead, vous devrez veiller à ce que le consentement de chaque individu concerné soit conforme au RGPD, ce qui veut dire que l'individu vous aura accordé son consentement clair et individuel pour que ses données soient vendues de cette manière. Compte tenu du fait qu'il est fort probable que la plupart des individus s'y refuseront, la vente et/ou le transfert de leads risquent fort de devenir des activités rares.

La minimisation des données

Le RGPD stipule que vous ne pouvez pas simplement obtenir des données auprès d'un individu sans justification (voir Respect de la vie privée dès la conception et par défaut en page 10). Vos procédés devront montrer de quelle manière vous recueillez les données et expliquer ce que vous avez l'intention d'en faire. En outre, il vous faudra obtenir un consentement pour utiliser ces données d'une manière spécifique. Il vous faudra également produire des documents indiquant quand vous avez l'intention de supprimer ou d'effacer ces données.

Traiter les demandes des clients

Comme il est mentionné en page 11, le RGPD donne à vos clients le droit de savoir ce que vous faites de leurs données. Ils ont également le droit de retirer leur consentement, sous réserve de certaines exceptions, ou le droit absolu de retirer leur consentement relatif à certaines utilisations de leurs données (comme le marketing direct). Vous devrez mettre en place des procédures et peut-être du personnel chargé de ces procédures, comme un DPO (voir en page 11). Votre personnel devra exécuter des tâches telles que la documentation de telles requêtes et la modification de certaines listes de marketing futures en fonction de la liste de suppression interne.

Les ressources humaines et la gestion de la paie

Étant donné que la gestion du personnel et de la paie implique le traitement d'énormes quantités de données à caractère personnel, il est fort probable qu'une révision importante de vos procédures existantes soit exigée dans le cadre du RGPD.

La consolidation et la sécurité

En vertu des exigences de sécurité supplémentaires, les entreprises doivent consolider toutes les données de leur personnel et des états de paie dans le moins d'emplacements possible pour se préparer au RGPD. Cela est dû à l'exigence en matière de sécurité des données (voir Respect de la vie privée dès la conception et par défaut en à la page 10). La sécurisation efficace des données à caractère personnel et/ou des données des états de paie relatives à la paie qui sont disséminées à travers un large éventail de feuilles de calcul Excel, par exemple, va probablement provoquer des catastrophes.

Les entreprises plus importantes devront également s'assurer qu'elles se conforment aux règles et normes pertinentes, comme l'ISO27001, et ceci devrait faciliter la mise en œuvre du RGPD.

Les processus conformes au RGPD que vous créez devront prendre en compte toutes les sources de données, ce qui peut s'avérer un véritable défi en termes de gestion du personnel. Par exemple, comment allez-vous stocker en toute sécurité des certificats d'arrêt de travail ou même des e-mails ou des SMS concernant des congés ? Comment les feuilles de présence peuvent-elles être gérées et stockées en toute sécurité ? Comment restreindre l'accès aux données à caractère personnel pour s'assurer que seules les personnes qui ont le « besoin de le savoir » peuvent y accéder ?

De manière similaire, et comme auparavant, les feuilles de paie doivent être fournies de manière sécurisée. Cela incite de nombreuses entreprises à se tourner vers la délivrance en ligne des feuilles de paie plutôt que l'envoie de feuilles de paie imprimées, ce qui implique que l'employé doit s'authentifier de manière sécurisée en ligne avant de pouvoir accéder à l'information.

Les droits individuels

Comme l'employé a conclu un contrat avec vous et que vous traitez ses données sur la base du contrat de travail ou pour vos intérêts légitimes, il n'est pas nécessaire approprié d'obtenir un consentement dans le cadre de la relation quotidienne employeur-employé. Vous pouvez néanmoins avoir besoin du consentement de l'employé pour tout traitement qui n'est pas directement lié à cette relation, par ex. si vous souhaitez consulter les dossiers de santé au travail d'un employé. Ceci implique le consentement en matière de données sensibles, bien que le RGPD se plie aux lois nationales sur ce point. Au moment de la rédaction, les implications à cet égard ne sont pas entièrement comprises.

Le RGPD signifie que vous devez potentiellement accorder à votre personnel une pleine visibilité des données que vous détenez à leur égard. Vous devez répondre aux demandes d'accès des sujets (subject access requests : SAR en anglais). Il est à noter que vous conservez le droit de refuser des demandes infondées ou excessives, mais vous devrez démontrer de quelle manière elles sont infondées dans votre documentation de conformité.

Vous devrez créer des avis de confidentialité clairs et conformes au RGPD pour vous assurer que vous fournissez toutes les informations auxquelles les sujets ont droit en vertu de l'exigence du RGPD en matière de transparence. Il vous faudra peut-être fournir une fonctionnalité facile d'accès pour permettre aux employés de se soustraire à diverses manières dont vous utilisez leurs données. Vous ne pouvez pas utiliser leurs données pour n'importe quelle finalité sans les en informer.

Le recrutement

À partir du moment où un employé potentiel soumet un curriculum vitae (CV) ou un formulaire de candidature, vous devrez commencer à enregistrer quand et comment vous obtenez ces données et en vertu de quelle base juridique vous les conservez.

Les CV reçus dans le cadre de candidatures spontanées soulèvent également des questions, étant donné que les services RH ne pourront pas les conserver à moins qu'ils ne puissent les relier à un enregistrement clair du consentement incluant un délai préalablement convenu. Il serait bon de réfléchir à la procédure impliquant de réclamer le consentement explicite du candidat pour conserver son CV pendant un certain délai. Comme susmentionné, il vous faudra également fournir des avis conformes au RGPD clairs aux demandeurs d'emploi.

La suppression des données

Le RGPD stipule que vous ne devez pas conserver les données d'un employé après son départ à moins que vous n'ayez une raison une raison légitime de le faire. Ceci doit être considéré dans le cadre du droit à l'oubli, comme il est mentionné en page 11 (voir Droits de vos clients), mais ceci n'est pas un droit absolu s'il existe une raison légitime pour que vous conserviez les données. Par exemple, si un ancien employé vous attaque en justice et saisit le Conseil des Prud'hommes, vous aurez alors besoin de conserver ces données.

Toutefois, vous devrez vous assurer que vos systèmes et vos procédures permettent la suppression de toutes les données de l'individu concerné, ce qui suggère une autre raison d'envisager la consolidation des données sur le moins de systèmes que possible.

La comptabilité et les finances

De tous les services au sein d'une entreprise, le service de la comptabilité est probablement le moins affecté par les préparatifs au RGPD et les exigences de ce dernier. En règle générale, les données de comptabilité ne devraient poser aucun problème à moins qu'elles ne soient liées à un individu.

Si vos données de comptabilité sont liées à un individu, dans la plupart des cas vous serez déjà engagé par contrat avec lui (par exemple, un contrat de vente) et, à des fins de comptabilité, vous traiterez les données pour leur intérêt légitime et le vôtre.

S'il est nécessaire d'obtenir un consentement pour utiliser les données d'un individu, l'exigence pour le traitement de ces dernières à des fins de comptabilité devrait alors être spécifiée au cours du processus d'obtention du consentement. Ceci pourrait impliquer que la personne ou l'équipe comptable communique avec tous les services pour s'assurer que la conformité au RGPD est respectée plus en amont au sein de l'entreprise.

Des problèmes peuvent éventuellement survenir si vous employez un comptable indépendant ou un cabinet comptable à quelque titre que ce soit. Vous devez vous assurer de leur conformité au RGPD, que la technologie et les logiciels qu'ils utilisent sont conformes au RGPD, et que la manière et l'endroit où ils stockent les données sont également conformes au RGPD.

Informatique

Les services d'informatique sont les facilitateurs d'une grande partie de la conformité au RGPD, étant donné que, de nos jours, la majorité du travail au sein d'une entreprise est effectuée via à l'aide de la technologie. Par exemple, avec l'utilisation croissante de services cloud, le service d'informatique devra s'assurer que l'emplacement où sont stockées les données est conforme à la sécurité réclamée par le RGPD.

Toutefois, ceci ne se limite pas nécessairement à la fourniture de logiciels et de matériels conformes au RGPD. Le service d'informatique pourrait être amené à se débarrasser en toute sécurité de données existantes, telles que les bases de données client qui ne sont pas couvertes par des avis de consentement adéquat, et à mettre en place des méthodes continues pour la suppression des données en toute sécurité afin de se conformer aux lignes directives bien plus strictes du RGPD en matière de conservation et d'utilisation des données.

Le service d'informatique devrait également prendre l'initiative en mettant en œuvre des processus robustes pour le reporting de violations de données ou d'autres formes de non-conformité au RGPD. Étant donné que ceci pourrait impliquer de contacter les clients (voir page 11), le service d'informatique devra communiquer avec tous les services pour s'assurer qu'ils comprennent les exigences du RGPD en matière de reporting.

Comme auparavant, la duplication de données à des fins de test et de pré-production est affectée par le RGPD car leur utilisation ne serait pas possible sans consentement explicite.

« De plus petites entreprises ont souvent une idée plus précise de leurs activités et peuvent donc remonter à la source, ce qui leur permet de savoir par où commencer à procéder aux modifications nécessaires. C'est un avantage.

Cependant, la conformité qu'elles doivent maintenant gérer est une charge de travail supplémentaire qu'elles n'ont probablement pas envisagée. Elles ne sont pas habituées à un tel niveau de gouvernance.

Je pense que de nombreuses sociétés ont été bien surprises du fait de devoir documenter et approuver tant de documents afin de pouvoir démontrer qu'elles font ce qu'elles disent faire. »

Se conformer avec exactitude au RGPD pourrait en fait prendre beaucoup de temps. Est-ce la manière dont une société fait bien les choses ? Doit-elle continuer de le faire de cette manière ? Tout ceci pourrait signifier impliquer l'affinement, voire même le changement, de procédures commerciales majeures. Il est parfois plus facile de reconcevoir le système et de trouver un meilleur moyen de le faire.

David Clarke

(FBCS CITP), fondateur du GDPR TechnologyGroup

RÉPONSES AUX QUESTIONS SUR LE RGPD

Voici des réponses aux questions fréquemment posées par les entreprises mettant en œuvre le RGPD.

Est-ce que mon entreprise doit devenir « certifiée RGPD » ?	Non. Le libellé du RGPD ne spécifie pas ni ne rend obligatoire un système de certification particulier, mais encourage la certification volontaire via des organisations ou organismes ou industriels conformes à l'EN-ISO/IEC 17065/2012 et qui ont été autorisés par les autorités de contrôle pertinentes, comme la CNIL en France.	Bien que la certification RGPD soit encouragée pour fournir des garanties relatives aux mesures de sécurité techniques et organisationnelles, entre autres, l'obtention de la certification est particulièrement importante pour les tiers qui traitent des données pour le compte d'autrui (appelés processeurs de données, voir page 8).
Mon entreprise vend ou fournit des services directement aux sociétés, mais pas aux particuliers. Est-ce que le RGPD m'affecte ?	Quasi certainement. Par exemple, si vous envoyez un e-mail à un individu d'une société pour organiser la vente d'un de vos produits ou services, le fait de connaître leur adresse e-mail signifie que vous recueillez des données d'identification à son propos en vue d'une activité économique.	Il est impossible d'imaginer une situation professionnelle pour laquelle de telles données ne sont pas générées et/ou recueillies, même par inadvertance. En outre, le RGPD a également un impact sur votre entreprise de manière interne. Il gouverne la façon dont vous gérez les données du personnel et la paie, par exemple (voir page 21).
Je suis autoentrepreneur. Est-ce que le RGPD m'affecte ?	Oui. Le RGPD affecte quiconque impliqué dans une activité économique et dans le traitement de données à caractère personnel, et ce, même pour des organisations telles que	des partenariats, des œuvres caritatives ou des clubs/associations. Peu importe que cette entité soit reconnue légalement ou non.
Est-ce que mon entreprise sera soumise à des audits RGPD ou des inspections ?	Le RGPD ne formule aucune exigence en matière d'inspections ou d'audits gouvernementaux réguliers, mais les autorités de contrôle comme la CNIL en France ont le droit de procéder à des audits dans le cadre de leurs pouvoirs d'enquête. Toutefois, cela ne veut pas dire que des audits ou des inspections auto-imposés ne sont pas une bonne idée ou même une exigence de facto pour la conformité au RGPD. Pour les tiers fournissant des services de traitement des données à autrui, la situation est un peu plus compliquée. Ils doivent également autoriser et contribuer à des audits, y compris des inspections, pour prouver que l'entreprise qui les emploie est mandatée.	Néanmoins, le RGPD introduit de nouvelles exigences importantes et onéreuses pour la tenue des registres, et ce, pour toutes les entreprises. Il ne suffit pas de seulement se conformer au RGPD. Toute entreprise doit être en mesure de le prouver. En plus des documents montrant vos procédures et plus encore, il se peut que vous ayez à prouver que vous appliquez un système de formation correct. Il est à noter qu'il est possible que les gouvernements mettent en œuvre des procédures d'audit régulières et officielles lors de l'intégration du RGPD aux lois nationales.

Pour quelle raison le RGPD est-il introduit alors que des lois sur la protection des données existent déjà ?	L'objectif est principalement de mettre à jour les lois sur la protection des données par rapport aux technologies modernes et aussi pour répondre aux attentes modernes des personnes. Il renforce également les droits des sujets des données de manière significative. Le champ de la protection des données a été élargi. Par exemple, on peut noter l'inclusion d'éléments tels que les données de localisation qu'un smartphone peut recueillir, ou les données génétiques et biométriques, mais sont également inclus des types supplémentaires et nouveaux de données qui peuvent être utilisées pour identifier un individu, comme leur origine culturelle ou sociale.	De plus, le RGPD ne se limite pas à la manière dont les entreprises devraient protéger les données. Il octroie aux individus de nouveaux droits importants quant aux données que vous détenez sur eux, et ceci pourrait également signifier un travail et une préparation supplémentaires pour votre entreprise. Les individus obtiennent aussi de nouveaux droits leur permettant de déposer des recours collectifs en cas de violation des données.
Les produits de Sage sont-ils prêts pour le RGPD ?	Sage travaille pour s'assurer que tous ses produits actifs respectent le RGPD. Plus spécifiquement, afin d'aider les organisations à respecter les obligations du RGPD, Sage continue à fournir des améliorations supplémentaires et il est donc conseillé aux clients de vérifier périodiquement la dernière version disponible et d'installer les mises à jour en fonction des besoins.	Les clients utilisant des produits Cloud, comme ceux du Sage Business Cloud, vont bénéficier du fait de toujours utiliser les dernières versions du logiciel.
Je suis déjà en conformité avec la loi informatique et libertés de 1978. Ai-je besoin de faire quoi que ce soit ?	Probablement. Le RGPD supplante toutes les lois gouvernementales existantes relatives à la protection des données pour les états membres de l'UE.	Notamment, étant donné que le RGPD est un règlement européen, il a toujours préséance sur la législation nationale d'un pays. D'un autre côté, il est possible que la loi informatique et libertés de 1978 inclut des éléments qui ne sont pas déjà dans le RGPD.

Combien le RGPD va-t-il coûter à mon entreprise ?

Les frais encourus pour une entreprise moyenne vont vraisemblablement inclure certains des frais suivants, sinon tous :

- Modifications telles que le recyclage du personnel et les adaptations informatiques
- Désignation potentielle et formation éventuelles d'un délégué à la protection des données (DPO ; voir ci-dessous)
- Mise en place et maintien de procédures de documentation continues démontrant la conformité au RGPD
- Coûts de certification volontaire, en particulier si votre entreprise traite des données pour le compte d'autres sociétés. Vous ne devez utiliser que des organismes de certification qui ont été autorisés par les autorités de contrôle pertinentes, comme la CNIL en France.

Mon entreprise n'est pas basée dans L'UE. De quelle manière suis-je affecté, le cas échéant ?

Le RGPD affecte toute entreprise à travers le monde qui traite les données d'individus de l'UE (voir Élargissement du champ et de la zone géographique en page 10). En fait, si vous proposez des produits ou services à des individus de l'UE ou si vous effectuez un suivi de leur comportement, vous devrez probablement employer un représentant dans l'UE pour gérer les requêtes liées au RGPD.

De plus, vous devez informer l'autorité de contrôle par écrit de qui il s'agit. De nombreux tiers se spécialisent déjà dans la gestion de cette exigence de représentation et vous pouvez les trouver en ligne. À tout le moins, vous devez vous renseigner pour savoir s'il s'agit d'une exigence pour votre entreprise.

Avant la mise en vigueur du RGPD, il est difficile de prédire les conséquences pour les entreprises évoluant hors de l'UE et qui contreviennent au RGPD, mais il se pourrait qu'on leur interdise d'effectuer des transactions commerciales dans l'UE jusqu'à ce que la conformité soit démontrée, ce qui pourrait prendre du temps.

Ceci pourrait affecter non seulement les ventes, mais également les fournisseurs et, par conséquent, avoir un effet dévastateur.

#IProtectData

Partagez le message. Partagez la responsabilité.

Au sein de Sage, nous comprenons que nos produits et services peuvent faire partie de contrôles et procédures que les entreprises doivent mettre en place pour se conformer à leurs propres obligations RGPD. Nous apportons notre soutien dans ce domaine en réexaminant tous nos produits et la documentation de soutien aux utilisateurs, ou en proposant des mises à jour des dernières versions supportées pour les clients. Ceci signifie que nous réalisons des avancées technologiques supplémentaires au niveau de nos produits pour nous assurer que nous sommes à la pointe en termes de portabilité des données, de tenue des registres et de droit à l'effacement au fur et à mesure du développement du RGPD.

Pour plus d'informations sur le RGPD et savoir ce que Sage fait pour que ses solutions soient prêtes :

rendez-vous sur: **www.sage.com/fr-fr/rgpd** >