RGPD

Guide pour les comptables et experts-comptables

www.sage.com/fr-fr/experts-comptables

Sommaire

Introduction

Une étude récente menée par Sage[1] montre que 60% des entreprises françaises ne connaissent pas suffisamment le Règlement général sur la protection des données (RGPD), alors que 57% ne comprennent pas quelles sont les implications du RGPD sur leur activité. Le RGPD va être mis en application dans quelques mois, il faut donc dès maintenant se préparer afin d'être en conformité avec la nouvelle réglementation dès le 25 mai 2018.

Chez Sage, nous estimons que ce niveau d'incertitude chez les experts-comptables et les petites et moyennes entreprises qui forment la base de leurs clients, signifie que de nombreux cabinets sont probablement mal préparés à gérer les conséquences du RGPD sur leurs activités et leurs clients.

Ce guide vous offre des informations claires sur les éléments du RGPD qui ont le plus d'importance pour vous, et leurs conséquences sur la façon dont vous menez vos activités avec vos clients. Nous voulons lever les malentendus qui pèsent sur les principaux éléments du RGPD en vous offrant des conseils pratiques et réalisables pour que vous soyez prêt pour le RGPD et soyez préparés à offrir des avis fiables à vos clients.

1. *Enquête clientèle Sage RGPD, 2017, France, 30 personnes interrogées.

RGPD : le point de vue de Sage

Adam Prince, VP Global Product Management

Sage s'engage à mettre en conformité toute sa gamme de produits ; aider les experts-comptables à se préparer au RGPD en est une des pièces maîtresses. Nous avons développé des procédures de gouvernance solides en vue de gérer la mise en place du RGPD dans notre entreprise afin de nous conformer à nos obligations et nous assurer que nous sommes prêts avant son application par l'UE le 25 mai 2018.

Nous partageons également nos connaissances et notre expertise avec la communauté des experts-comptables dans le cadre d'un programme externe déjà en cours. Nos offres de formations, que ce soit les webinaires, les événements Sage, notre collaboration dans le cadre d'une initiative de formation de clients, sont conçues pour vous aider à être prêt pour le RGPD et vous permettre de donner des conseils avisés à vos clients.

Cameron John, Global Director of Accountant Partners

Le GDPR modifie profondément la façon dont les experts-comptables travaillent et interagissent avec leurs clients. Les experts-comptables, considérés comme des sources de conseils et d'informations fiables, notamment pour les petites et moyennes entreprises, ont l'opportunité de jouer un rôle crucial et d'aider leurs clients à se préparer et se mettre en conformité avec le RGPD.

L'incertitude liée aux changements législatifs expose également les lacunes de connaissances et de compréhensions qui peuvent avoir des conséquences sur les conseils offerts. Chez Sage, nous nous concentrons sur notre collaboration avec les experts-comptables pour lever les incompréhensions grâce à des conseils et des mesures pratiques qui vous permettent de vous préparer au RGPD.

Nous sommes également là pour aider votre cabinet à réaliser son potentiel de développement et à atteindre le succès grâce à une transformation numérique. Orienter vos clients vers des logiciels de comptabilité sur le cloud est une véritable opportunité à saisir pour votre cabinet, en termes d'amélioration des performances, mais aussi en termes de développement de vos services afin d'apporter encore plus de valeur ajoutée à vos clients.

Grâce à des outils innovants, comme ce guide, nos événements Sage et des supports d'exercices, nous partageons notre expertise afin de vous fournir toutes les connaissances afin que vous répondiez mieux aux besoins de vos clients. Ensemble, nous pouvons faire du défi du RGPD une opportunité.

RGPD : le point de vue d'un expert-comptable

Chris Downing, Business Intelligence Partner, Milsted Langdon LLP

En tant qu'experts-comptables, notre activité est souvent régie par des méthodes et processus standardisés. Si cela signifie que nous sommes capable de repérer les problèmes dans les détails, nous pouvons également nous retrouver coincés dans nos procédures et nos méthodes de travail. Ce sentiment s'applique à la façon dont notre profession traite les données, en particulier en ce qui concerne notre responsabilité sur leur collecte, stockage et utilisation appropriés, que ce soit pour notre cabinet ou pour nos clients.

Le RGPD est une opportunité de changer la façon dont nous voyons les données personnelles et dont nous les utilisons. En voulant servir nos clients de la manière qui leur convient le mieux, tout en prenant en compte nos propres préférences sur la gestion de nos activités, nous avons créé une mosaïque de moyens de collecter, gérer et distribuer les données : des fichiers papiers, des feuilles Excel, des logiciels, des archivages numériques localisés, etc. Notre profession doit en faire table rase et le RGPD est une bonne opportunité de modifier et d'adapter nos procédures de travail.

Chez Milsted Langdon, nous voyons le changement législatif du RGPD comme une chance de collaborer avec nos clients et d'implanter notre expertise chez eux en étant considérés comme des conseillers fiables. Nous leur offrirons bien sûr toujours les services quotidiens qui leur sont nécessaires. Pour se préparer à la conformité au RGPD, nous impliquons tout notre cabinet afin que, tous ensemble, nous comprenions mieux quelles sont nos responsabilités en tant qu'experts-comptables. Nous sommes, entre autres, responsable de :

- **Identifier les acteurs clé au sein de tous les départements pour comprendre quelles données nous gérons au quotidien.**
- **Comprendre le type de logiciels que nous utilisons, s'ils sont sur site ou sur le cloud, et les considérations techniques qui y sont liées.**
- **Faire le point sur nos fournisseurs externes de services externalisés afin de s'assurer qu'ils sont en conformité en tant que sous-traitants.**

Cette approche nous permet de créer une communauté interne qui prend en charge la responsabilité globale de notre préparation pour le RGPD en mettant en commun les compétences et l'expérience de chacun tout en allant chercher une expertise externe.

Les autres sociétés qui veulent se préparer pour le RGPD doivent absolument comprendre ce que ces directives impliquent dans la pratique dans leur cas précis. Il s'agit de savoir ce qu'il faut changer dans vos activités quotidiennes par rapport à la façon dont vous gérez les données personnelles, et quelles sont les solutions appropriées pour que votre entreprise y soit conforme.

Le guide pratique de Sage contribue à faire le point sur toutes ces questions et offre un point de vue pratique.

Qu'est ce que le RGPD ?

Le RGPD est la nouvelle législation qui encadre les données personnelles. Il entre en application dans l'Union européenne à compter du 25 mai 2018. Les réglementations européennes ont un effet direct sur tous les états membres, ce qui signifie que le RGPD va prendre le pas sur les législations nationales. Aucun délai de grâce n'est prévu.

Le RGPD a pour vocation de protéger les données à caractère personnel, c'est-à-dire les données des particuliers. Dans les faits, le RGPD est l'un des plus grands bouleversements jamais connu qui affecte la façon dont les données relatives à un individu sont gérées. Il a des conséquences non seulement sur les entreprises, mais également sur les individus, corporations, autorités publiques, agences et toute entité qui traite des données personnelles d'individus établis dans l'UE. Cela inclut les prestataires auxquels une entreprise pourrait faire appel pour le traitement de données à caractère personnel.

Le périmètre d'application de ce règlement est remarquablement large car il inclut tous les états membres de l'Union européenne. À l'inverse de la directive européenne 95/46 sur la protection des données, le RGPD s'applique également aux entreprises hors de l'UE qui proposent des biens et des services aux individus basés dans l'UE, ou qui surveillent leur comportement au sein de l'UE. Les entreprises dont les sites internet sont hébergés aux États-Unis, mais sont accessibles aux résidents de l'UE sont donc directement affectées.

Le RGPD a des implications majeures pour tous les départements de nombreuses entreprises dans le monde entier, à tel point que certaines doivent embaucher un délégué à la protection des données pour y faire face, et que la grande majorité doivent mettre en place de nouvelles pratiques et mesures de protection.

Il est hautement recommandé de faire appel à quelqu'un ayant les qualifications requises pour effectuer un audit, et connaître les implications du RGPD devrait être considéré obligatoire en raison du montant des amendes encourues, jusqu'à 4% du chiffre d'affaires ou 20 millions d'euros, le montant le plus élevé étant retenu.

Règlement général sur la protection des données (RGPD)

Droits individuels

Augmente énormément les droits des individus et quelles informations ils peuvent obtenir en ce qui concerne les activités qui utilisent leurs données

Consentement

Doit être confirmé par une déclaration ou une action affirmative claire

Délégué à la protection des données

Doit être un expert dans le domaine de la législation sur la protection des données

Sanctions

Jusqu'à 4 % du chiffre d'affaire annuel ou 20 millions d'euros le montant le plus élevé étant retenu

La confidentialité du début à la fin

Le prise en compte du respect de la vie privée doit être intégrée partout et seules les données strictement nécessaires pour le but indiqué peuvent être utilisées

Portabilité des données

Les individus ont maintenant le droit de déplacer, copier ou transférer leurs données personnelles - même à un concurrent

Champ d'application étendu

Protégez votre entreprise, ainsi que ceux qui traitent pour vous des données - même hors de l'UE

Notifications obligatoires en cas de fuite de données

Les responsables du traitement doivent alerter les autorités de surveillance locales dans les 72 heures

Le RGPD en résumé

Les points clé du RGPD, en particulier en lien avec la directive européenne actuelle 95/46 (la directive).

Les droits individuels, et comment en informer les individus

La directive actuelle donne des droits aux individus sur leurs données personnelles et décrit le type d'informations que les entreprises doivent leur fournir lorsqu'ils le demandent, y compris la façon dont l'entreprise compte utiliser leurs données personnelles. Cela se faisait auparavant via des déclaration de confidentialité ou des notifications sur un site internet.

Le RGPD pousse ce principe bien plus loin, en accordant des droits supplémentaires qui doivent à nouveau être communiqués. Les individus doivent, en particulier, être informés qu'ils ont les droits suivants (liste non-exhaustive) :

a) de se plaindre aux autorités de surveillance ; comme la CNIL en France;
b) retirer leur consentement pour le traitement de leurs données personnelles (voir ci-dessous) ;
c) accéder à leurs données personnelles et de les faire rectifier ou effacer (le 'droit à l'oubli') par les entreprises ainsi que d'obtenir les détails de tous les tiers ou catégories de tierces parties qui y ont accès ;
d) être informés de l'existence de toute utilisation automatisée des données personnelles (y compris le profilage) ;
e) refuser certains types d'utilisations, comme le marketing direct ou les décisions fondées uniquement sur le traitement automatisé ;
f) savoir pendant combien de temps leurs données personnelles vont être conservées ;
g) connaitre les coordonnées du délégué à la protection des données désigné (voir ci-dessous).

En outre, ils ont le droit de faire appel à des organisations à but non-lucratif pour exercer leurs droits et intenter des actions en justice en leur nom.

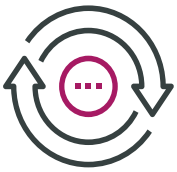
Consentement

Si vous recueillez des données sur le fondement du consentement des individus, bien que la législation européenne sur la protection des données ait toujours exigé que vous demandiez un consentement libre, spécifique et informé, le RGPD exige maintenant que ce consentement soit confirmé par une déclaration ou une action affirmative claire. En d'autres termes, des cases pré-cochées sur un site internet, ou l'absence de réaction ou le silence d'un individu après avoir lu une politique de confidentialité ne seront plus considéré comme un consentement.

Un consentement ne peut pas non plus être universel, donc une entreprise ne peut pas utiliser une seule autorisation de la part d'un individu à une étape de leurs interactions avec l'entreprise comme son consentement pour d'autres utilisations de leurs données personnelles. Des autorisations individuelles sont nécessaires pour chaque utilisation différente des données personnelles.

Pour finir, les individus doivent non seulement être informés qu'ils ont le droit de retirer leur consentement n'importe quand, mais ce doit également être aussi facile pour eux de retirer leur consentement que de le donner.

Les autorisations pré-existantes données par des individus doivent être réexaminées afin de s'assurer qu'elles répondent aux exigences du RGPD. En cas de conflit ou d'ambiguïté, les entreprises doivent soit établir une nouvelle base légale pour l'utilisation des données (dans le cas où cette utilisation est nécessaire pour l'exécution d'un contrat, par exemple), soit obtenir une nouvelle autorisation ou cesser d'utiliser ces données personnelles.



Le droit de déplacer ou transférer des données personnelles (droit à la portabilité)

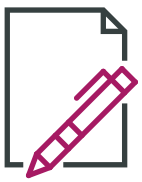
Lorsque des données personnelles ont été confiées à un responsable du traitement des données sur la base d'un contrat ou d'une autorisation, les personnes concernées ont le droit de déplacer, copier ou transférer leurs données personnelles d'un responsable à une autre, même à un concurrent.

Une entreprise peut, par exemple, travailler avec un cabinet d'experts-comptables attitré. Si elle décide de changer de fournisseur, elle peut récupérer toutes les données détenues par ce cabinet. Les données personnelles doivent donc être conservées et gérées dans un format structuré, couramment utilisé et lisible par machine afin d'être facilement utilisées et partagées.

Cette exigence de rendre les données vraiment portables et faciles à utiliser par d'autres entités va probablement provoquer des ajustements informatiques majeurs, et donc des coûts associés.

Champ d'application étendu

Pour dire les choses simplement, le RGPD rend responsable des infractions non seulement l'entreprise qui collecte les données, mais également les tiers éventuels qui utilisent ces données au nom de cette entreprise. Cependant, cela ne signifie pas qu'une entreprise peut simplement transmettre des données personnelles à un tiers et fermer les yeux. L'entreprise doit s'assurer que le fournisseur tiers est également en conformité avec le RGPD. Ceci est une menace potentielle pour les experts-comptables qui, généralement, traitent des données personnelles liées à leurs clients (en tant que responsable du traitement), ainsi que liées à leur propre activité (en tant que sous-traitants). Le champ d'application géographique a également été élargi au-delà de l'UE à toutes les entreprises ou tiers qui traitent des données personnelles en leurs noms. Comme l'UE est un partenaire économique de la plupart des pays, le champ d'application étendu du RGPD signifie qu'il affecte de nombreuses entreprises dans le monde entier. Elles devront donc se mettre en conformité avec le RGPD si elles souhaitent exercer leur activité dans les états membres de l'UE, que ce soit directement ou en tant que fournisseurs pour d'autres entreprises.



Preuve de conformité

Il n'est pas suffisant de simplement être en règle avec le RGPD. Une entreprise doit prouver qu'elle est en conformité avec les règles du RGPD concernant leur « responsabilité », ce qui implique de respecter des exigences onéreuses en matière de tenue de registres. Il faut, notamment, tenir des registres qui détaillent les utilisations des données*, les demandes d'accès, les infractions, la façon dont les autorisations sont obtenues et des études d'impact sur la vie privée. Les tierces parties qui traitent des données personnelles au nom d'autres entreprises sont également soumises à ces règles, même si les exigences ne sont pas aussi détaillées.

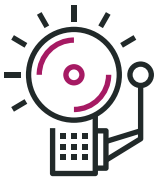
** S'applique aux entreprises de plus de 250 salariés, ou les entreprises de taille plus petite chez lesquelles l'utilisation des données personnelles est susceptible d'entraîner un risque pour les droits et libertés des individus, n'est pas occasionnelle, ou inclut des catégories spéciales de données, comme des informations sur la santé, la religion ou l'orientation sexuelle.*

La confidentialité du début à la fin

Les mesures de sécurité techniques et organisationnelles doivent être en place tout au long du cycle de vie des données personnelles afin de répondre aux attentes en matière du respect de la vie privée, de leur collecte à l'arrêt de leur utilisation, en passant par leur utilisation. On appelle cela la « protection des données dès la conception », ce qui signifie que la prise en compte du respect de la vie privée doit être intégrée à tous les aspects du processus.

En outre, seules les données personnelles strictement nécessaires doivent être collectées et utilisées C'est ce qu'on appelle parfois la limitation des données ou « sécurité par défaut ».

Mettre en œuvre la protection des données dès la conception et la sécurité par défaut nécessite une formation continue, la mise en place d'audits réguliers, la limitation des données collectées, la restriction des accès aux données personnelles selon le principe du « besoin de connaître », et l'application de mesures de sécurité techniques et organisationnelles appropriées comme la pseudonymisation et le cryptage des données.



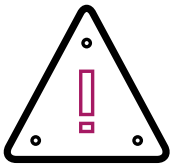
Notifications obligatoires en cas de fuite de données

En cas d'une fuite de données qui provoquerait probablement un risque pour les droits et libertés des individus, les entreprises qui ont collecté ces données personnelles doivent informer la Commission nationale de l'informatique et des libertés (CNIL) dans les 72 heures. Les fournisseurs tiers qui utilisent des données personnelles au nom d'autres entreprises doivent les prévenir en cas de fuite sans attendre.

Si ces fuites de données posent un risque élevé pour les individus concernés, les entreprises doivent également prévenir les individus concernés sans attendre.

Le délégué à la protection des données

Dans le cadre du RGPD, les entreprises qui utilisent des données personnelles (que ce soit en tant que responsable du traitement ou en tant que sous-traitant pour le compte d'un responsable du traitement) doivent nommer un délégué à la protection des données si : (i) il s'agit d'un organisme public ; (ii) si les activités principales d'une entreprise impliquent la surveillance des utilisateurs à grande échelle ; ou si ses activités principales consistent à traiter des catégories spéciales de données personnelles à grande échelle, notamment les données concernant les condamnations pour crimes et délits. Le délégué doit être un expert dans le domaine des lois sur la protection des données. Il ne doit pas nécessairement être un employé, mais peut être employé dans le cadre d'un contrat de service pour remplir ce rôle. Les coordonnées du délégué devront être communiquées à l'autorité de surveillance, comme la CNIL en France.

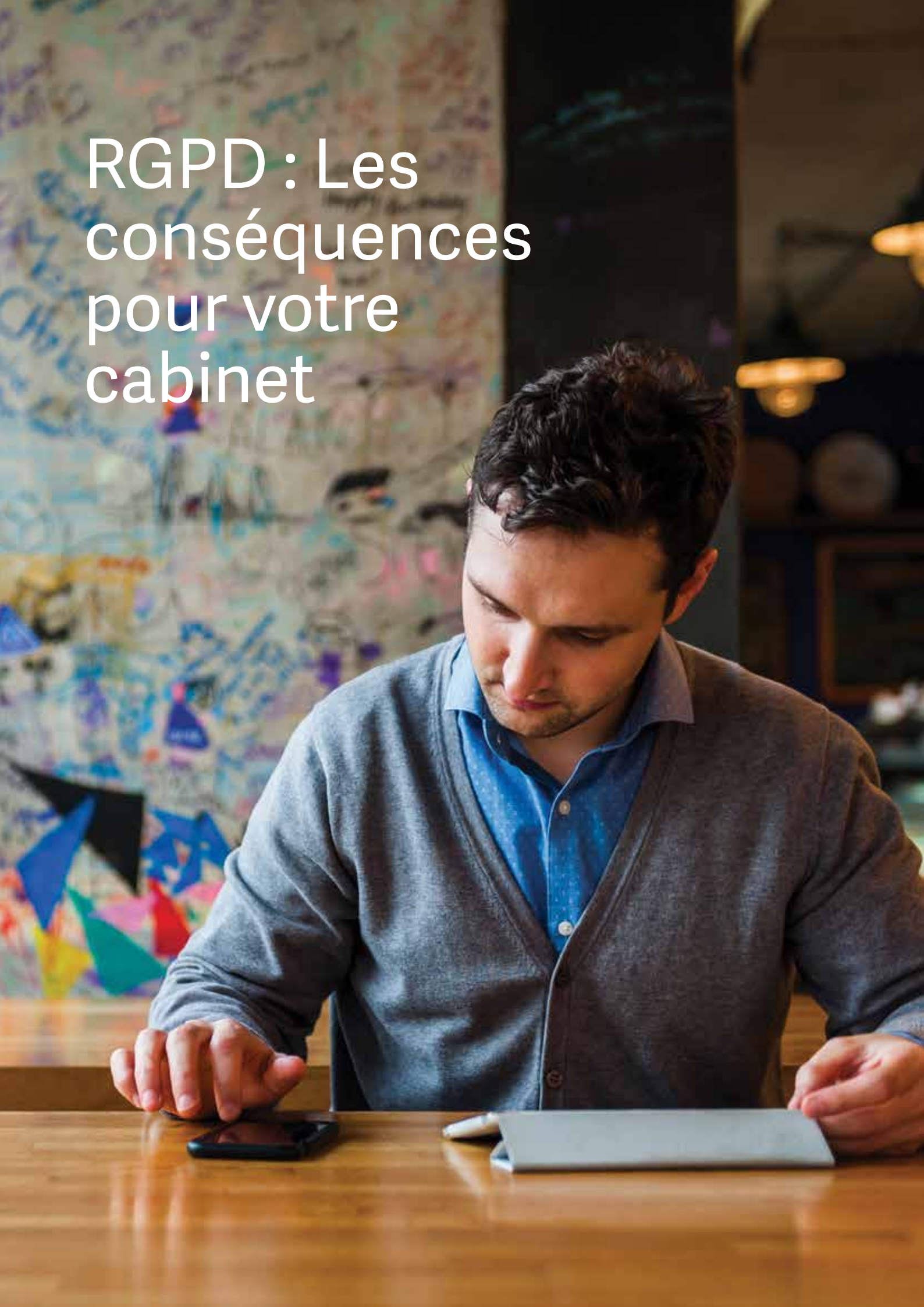


Sanctions

Les sanctions en cas de non-conformité avec le RGPD sont sévères et les amendes peuvent monter jusqu'à 4% du chiffre d'affaires mondial annuel ou 20 millions d'euros, le montant le plus élevé étant retenu. Vous pouvez recevoir une amende même si aucune donnée n'a été perdue.

Il faut noter qu'il n'y a pas d'exclusion ou d'exception pour les petites entreprises. En outre, les particuliers peuvent exercer un recours collectif afin de réclamer une enquête réglementaire formelle si une entreprise ne se conforme pas au RGPD.

RGPD : Les conséquences pour votre cabinet



Différencier les rôles

Il est primordial que vous compreniez quel est votre rôle en tant que cabinet d'experts-comptables dans le contexte du RGPD. Les experts-comptables et les comptables seront impliqués avec les données personnelles sous deux aspects :

1. **En tant qu'employeur : vous stockez, contrôlez et utilisez les données personnelles de vos employés**
2. **En tant que fournisseur tiers pour vos clients.**

Afin d'être en conformité avec le RGPD, chacun de ces rôles requiert de votre part un questionnement et une réflexion claire par rapport à la façon dont vous gérez, stockez et utilisez les données personnelles.

Le RGPD identifie deux rôles clairs qui déterminent les paramètres selon lesquels les données personnelles doivent être traitées :

Responsables du traitement des données

La personne physique ou morale, l'autorité publique, l'agence ou toute autre organisation qui, seule ou conjointement avec d'autres, détermine le but de l'utilisation des données personnelles et la façon dont cette utilisation a lieu. Si vous collectez des données personnelles pour votre propre utilisation et pour vos propres objectifs, vous êtes le responsable du traitement et êtes entièrement responsable de votre conformité avec le RGPD, y compris en termes de sécurité.

Sous-traitant

Une personne physique ou morale, autorité publique, agence ou toute autre organisation qui traite des données personnelles au nom du responsable du traitement. Si vous traitez des données personnelles au nom d'une autre organisation, vous être le sous-traitant et ne devez agir que selon les instructions de l'organisation qui est le responsable du traitement. Vous êtes également responsable des obligations de conformité au RGPD imposées aux sous-traitants.

Pour les experts-comptables et comptables, vous agissez en tant que « contrôleurs en commun » avec vos clients lorsque vous déterminez quelles informations vous devez obtenir et traiter afin de réaliser le travail qui vous a été confié. Cela va au-delà du rôle de sous-traitant, qui n'agit qu'au nom du responsable du traitement des données, en s'occupant de la paie, par exemple. Lorsque des comptables et experts-comptables sont identifiés en tant que responsables du traitement des données pour les données de leurs clients (via un accord de partage des données couvert par les termes et conditions), le RGPD indique qu'ils n'ont pas à fournir d'informations sur le traitement équitable des données lorsque celles-ci restent confidentielles en raison de l'obligation de secret professionnel. À l'heure où nous écrivons ces lignes, il semble qu'il n'est pas nécessaire d'informer les personnes concernées lorsque cela compromettrait la praticabilité et l'obligation de confidentialité. Cela doit toutefois être confirmé.

Le groupe de travail européen sur la protection des données a récemment clarifié un peu plus ce point :

La qualification d'un expert-comptable dépend du contexte. Lorsque les experts-comptables fournissent leurs services au grand public et à des petits commerçants sur la base d'instructions très générales (« Préparez mes déclarations de revenus »), il est alors un responsable du traitement des données, tout comme un avocat agissant dans des circonstances et pour des raisons similaires. En revanche, lorsqu'un expert-comptable est employé par une entreprise et reçoit des instructions détaillées de la part d'un comptable interne à l'entreprise, pour effectuer un audit détaillé, par exemple, il est en général, si ce n'est pas un employé standard, sous-traitant, en raison de la clarté des instructions et de son pouvoir limité d'appréciation qui en découle.
Cela repose toutefois sur une condition majeure. Dans le cas où ils considèrent avoir découvert une faute professionnelle qu'ils sont dans l'obligation de rapporter, ils agissent alors indépendamment en tant que responsables du traitement en raison de leurs obligations professionnelles.

Responsabilités en matière de données personnelles

Le RGPD fixe les exigences minimales de traitement des données personnelles. Les données personnelles peuvent être définies comme étant toutes les données qui permettent d'identifier un individu ou qui lui sont liées (y compris des éléments comme l'apparence physique ou même les données biométriques).

La plupart des entreprises commencent à collecter des données personnelles à la minute où elles commencent à interagir avec un individu, et dans la plupart des cas, n'ont même pas conscience qu'elles le font. Ainsi, collecter des données personnelles peut être aussi simple que d'utiliser des cookies qui identifient un utilisateur de votre site web, par exemple. Cela va jusqu'à avoir un dossier sur un individu dans un système de gestion des clients (CRM), et même bien au-delà. Même si les données personnelles sont collectées ou traitées au seul bénéfice de l'individu, cela rentre tout de même dans le cadre du RGPD.

Cela signifie que les cabinets comptables doivent repenser la façon dont ils collectent, gèrent et utilisent les données personnelles, pour eux et pour leurs clients. Étant donné le bouleversement provoqué par le RGPD, il est peu probable qu'une entreprise puisse s'y conformer sans apporter des ajustements à ses processus et procédures. Pour la majorité des entreprises, il est probable qu'il faille mettre en place des changements radicaux, et non pas quelques petites retouches.

Traiter les données des clients

Le RGPD offre six bases légales qui permettent de gérer et traiter des données personnelles :

1. **L'intérêt légitime :** Il s'agit d'un domaine subjectif et les sociétés doivent trouver un équilibre entre leur droit en tant qu'entreprise à utiliser des données personnelles et le droit des individus à ce qu'elles ne soient pas utilisées. Elles doivent justifier d'un besoin clair et impérieux à utiliser ces données personnelles. Il serait de bon aloi de documenter le raisonnement qui sous-tend cette décision. Ce principe s'applique également lorsque vous utilisez des données personnelles pour les besoins du marketing.
2. **Consentement :** Le consentement doit être obtenu de façon libre, informée et non ambiguë. Il peut être enregistré sous différentes formes (une case à cocher en ligne, par exemple) ou en répondant « Oui » au téléphone, et ce consentement doit être conservé dans les registres.
3. **Contrat :** Cela concerne l'utilisation des données personnelles dans le cadre d'un contrat dont la personne concernée par les données personnelles est une partie, ou les étapes qui précèdent la signature d'un contrat où des données personnelles doivent être rassemblées. Les réglementations actuelles de protection des données ne changent pas dans ce cas.
4. **Obligation légale :** Ce point est particulièrement important pour les cabinets comptables qui ont une obligation légale à conserver des données personnelles pars les réglementations financières, par exemple pour des raisons fiscales ou dans le but d'éviter des fraudes.
5. **Intérêts vitaux :** Une organisation peut devoir utiliser des données personnelles en vue de protéger les intérêts vitaux du sujet des données. Cela concerne en substance les cas de « vie ou de mort ».
6. **Intérêt public :** Ce point s'applique quand il faut traiter des données personnelles dans le cadre de l'intérêt public, comme dans le cas de tâches effectuées par une autorité publique, par exemple. Dans le cas des cabinets comptables, il peut s'agir de l'envoi à l'administration fiscale des détails des salaires des employés ou des clients en vu du calcul des impôts.

À propos des logiciels

Les logiciels comptables sont cruciaux pour de nombreuses entreprises qui utilisent des données financières et personnelles pour le compte de leurs clients. Dans le cadre de l'application du RGPD, il faut prendre en compte techniquement comment et où votre logiciel traite et héberge les données personnelles, tout particulièrement s'il est sur le cloud.

Les comptables et experts-comptables doivent vérifier auprès de leurs fournisseurs informatiques et fournisseurs de logiciels la conformité de leurs systèmes avec le RGPD. Une liste de vérification ou un questionnaire complet vous aidera à connaître les flux de données et à identifier les points de vulnérabilité avant la date de mise en place du RGPD. Cette liste ou ce questionnaire doit couvrir tout ce qui concerne la façon dont le logiciel interagit avec des données personnelles, notamment, mais pas uniquement :

- **Les spécifications techniques de la plateforme**
- **La séparation des données**
- **L'utilisation des techniques d'anonymisation, de pseudonymisation et de chiffrage**
- **La sécurité, en prenant en compte les appareils mobiles**
- **La désactivation des données**
- **L'externalisation/la sous-traitance**
- **Les sauvegardes et procédures de reprise après sinistres.**

Données utilisées pour le marketing

Le consentement et l'intérêt légitime sont des considérations primordiales lorsqu'il s'agit d'évaluer l'utilisation de données personnelles à des fins marketing. Avez-vous le consentement d'un individu et est-ce pour ce but que vous avez reçu son consentement ? Lorsqu'il s'agit de contacter un individu pour une raison qui n'est pas celle pour laquelle il a donné son consentement, l'intérêt légitime doit être prouvé. Par exemple, l'intérêt légitime peut être invoqué dans les cas où vous contactez vos clients à propos d'un nouveau service offert par votre entreprise, car il est dans leur intérêt d'être mis au courant de cette information.

Coordonnées des prospects

Il est courant dans les cabinets comptables de conserver les détails de tous les contacts établis par des clients potentiels, notamment leurs coordonnées et la nature de leurs demandes. Ils sont ensuite utilisés pour mener des propositions de missions commerciales, dans le but de convertir ces prospects en clients. Après l'entrée en vigueur du RGPD, les cabinets devront chercher sur quelle base légale ils pourront conserver ces données et quel accord ils ont reçu pour leur utilisation, que ce soit via un consentement, un contrat ou un autre intérêt légitime. Pour de nombreux comptables et experts-comptables, cela va impliquer un changement de procédure qu'il faudra prendre en compte dans le plan de mise en conformité avec le RGPD.

Données des fournisseurs

Après avoir réfléchi à la façon dont vous traitez les données personnelles de vos clients et employés, vous ne devez pas oublier celles de vos fournisseurs. Il est tout à fait possible que vous receviez des données personnelles dans le cadre de ce type de relation, or ces données doivent faire l'objet du même niveau de protection que celles des autres individus.

En outre, si vos fournisseurs sont chargés de traiter des données personnelles en votre nom, n'oubliez pas que le RGPD exige que certaines dispositions soient incluses dans les accords écrits qui vous lient à ces fournisseurs. Si la situation est inversée et que vous êtes sous-traitant pour le compte d'une autre organisation, vous devez vous attendre à devoir également intégrer de nouvelles conditions de traitement des données.

Données des employés et recrutement

Le RGPD accorde plus de droits aux employés en tant que sujets des données. Ces droits incluent :

- **Le droit d'être informé, qui inclut l'obligation pour l'employeur d'assurer la transparence sur la façon dont les données personnelles vont être utilisées.**
- **L'accès aux données, qui inclut les demandes d'accès effectuées par leur sujet.**
- **La rectification des données inexactes ou incomplètes.**
- **Le droit à l'oubli (dans certaines circonstances).**
- **Le droit de bloquer ou supprimer l'utilisation de données personnelles.**
- **La portabilité des données, qui permet aux employés d'obtenir et de réutiliser leurs données personnelles, par exemple lorsqu'ils rejoignent une autre entreprise et qu'ils demandent que leurs données personnelles soient transférées.**

L'autre aspect important que les cabinets comptables doivent prendre en compte est le recrutement. Avant l'entrée en vigueur du RGPD, il est assez courant de la part des cabinets de conserver des copies des CV reçus une fois le poste pourvu au cas où l'un des candidats correspondrait à un autre emploi. Après son entrée en vigueur, ceci ne sera plus possible à moins qu'un accord express n'ait été demandé et donné, auquel cas les données doivent être stockées et gérées selon les règles édictées par le RGPD.

Coûts de mise en conformité

Les cabinets comptables doivent identifier les coûts liés aux nouveaux systèmes, processus et ressources nécessaires à la mise en conformité avec le RGPD et s'organiser en conséquence. Cela peut inclure le passage de la tenue de dossier sur papier à l'utilisation d'un logiciel, ce qui implique non seulement d'investir dans le système, mais aussi de mettre en place une formation suffisante pour les employés et clients.

Inspirer confiance

Les experts-comptables sont des conseillers appréciés et fiables pour leurs clients. Afin de répondre à ces attentes, il est primordial qu'ils partagent leurs connaissances avec leurs clients et les conseillent correctement à propos des législations importantes. Il est à présent temps d'analyser et de comprendre les implications probables du RGPD sur votre activité et vos clients.

Protéger les droits à la confidentialité des données personnelles

La protection des données personnelles, une fois le RGPD entré en vigueur, sera bien plus stricte, en particulier en ce qui concerne les données obtenues via des sites internet. Par exemple, il faudra rendre parfaitement explicite le moment où un utilisateur s'inscrit à un service via des cases à cocher ainsi que ce à quoi ces cases correspondent. Toute contamination des données personnelles, c'est-à-dire à chaque fois qu'un individu est contacté dans un cadre pour lequel il n'a pas donné son consentement, pourra être reportée comme atteinte à la protection des données personnelles.

Échange de données des clients

Vous devez évaluer et cartographier la façon dont vous gérez les données personnelles, mais également la façon dont vous échangez ces éléments. Il s'agit là d'une des points fondamentaux de votre préparation pour la mise en conformité avec le RGPD. Dans le cadre du RGPD, les clients ont le droit d'auditer les tiers agissant comme sous-traitants afin de s'assurer de la conformité de l'ensemble de leur chaîne d'approvisionnement.

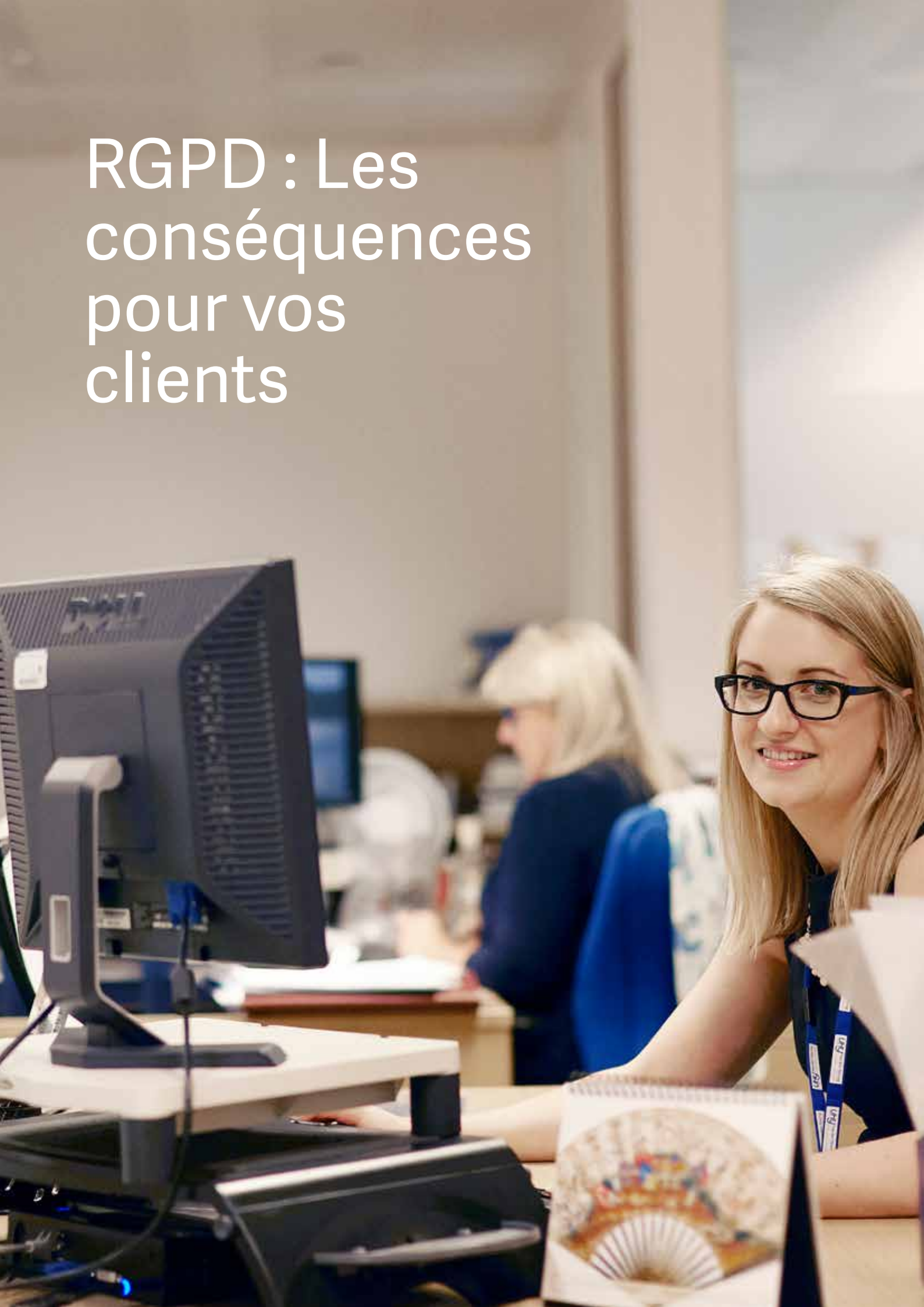
Le RGPD contient des exigences prescriptives à propos du partage de données entre le responsable du traitement des données et le sous-traitant. Par exemple, le sous-traitant doit maintenant :

- **Tenir à jour des registres de toutes les activités de traitement effectuées au nom du responsable du traitement, s'il s'agit d'une entreprise de 250 salariés et plus. Les autres entreprises sont également concernées lorsque l'utilisation qui est faite des données présente un risque pour les droits et libertés des sujets des données, ce traitement n'est pas occasionnel ou qu'il inclut des catégories spéciales de données ou des données personnelles telles que les condamnations pour crimes et délits.**
- **Obtenir le consentement du responsable du traitement pour nommer un sous-traitant ultérieur.**
- **Coopérer avec le responsable du traitement à l'égard du respect de ses obligations en vertu du RGPD, y compris prévenir sans délai le responsable du traitement des données de toute faille de sécurité concernant les données personnelles.**

En conséquence, les clients des experts-comptables (en tant que responsable du traitement) vont vouloir examiner leurs accords présents et futurs afin de s'assurer que ces exigences soient respectées. Quand votre cabinet agit en tant que « contrôleur en commun » avec vos clients, vous devez prendre en considération les points suivants lorsque vous mettez en place un accord de partage des données :

- **Clarifier les raisons de ce partage.**
- **Indiquer quelles données vont être partagées.**
- **Confirmer la base des données partagées.**
- **Détailler les limites imposées aux destinataires des données partagées**
- **Valider la qualité, la sécurité et la conservation des données.**
- **Vérifier le processus afin d'assurer une gestion pratique.**

RGPD : Les conséquences pour vos clients



Les dirigeants de petites et moyennes entreprises visent souvent à s'assurer que leur entreprise est stable et prospère, ce qui signifie qu'ils s'appuient fortement sur les avis et conseils de leur réseau. En tant qu'experts-comptables, vous êtes au cœur de ce réseau et vous pouvez apporter vos connaissances et votre expertise à vos clients pour les aider à affronter les changements majeurs de réglementation, comme la mise en place du RGPD.

En passant en revue quelques points simples avec vos clients, vous pourrez les aider à comprendre les conséquences probables du RGPD sur leur entreprise et comment ils peuvent transformer ce qu'ils perçoivent comme un défi en opportunité.

En vous concentrant en premier lieu sur des questions essentielles, vous pourrez prioriser les points de discussions et établir le niveau de compréhension de vos clients, ainsi que l'aide dont ils auront probablement besoin, notamment les conseils opérationnels, financiers et légaux. Les questions à poser à vos clients à propos du RGPD incluent :

- **Que comprennent-ils du RGPD ?**
- **Dans quelle mesure ont-ils cartographié toutes les procédures utilisées dans leur entreprise qui impliquent des informations personnelles ? Leur inventaire des données personnelles est-il exhaustif : leurs registres sont-ils conservés de façon centralisée, qu'ont-ils au format papier et au format numérique, qui a accès aux données ?**
- **Quelle action immédiate est nécessaire pour rectifier les problèmes qui peuvent se poser en termes de stockage des données, du type d'informations conservées et de responsabilité des données ? Ce point doit se concentrer sur tous les aspects qui ne sont pas conformes au RGPD.**
- **Comment s'assurent-ils que leurs fournisseurs et partenaires sont en conformité, y compris leur expert-comptable ?**
- **Comment comptent-ils désigner un responsable de la conformité au sein de leur entreprise et s'assurer que leurs employés connaissent le RGPD et peuvent se conformer à la nouvelle réglementation ?**

En établissant avec vos clients un plan afin de s'assurer qu'ils sont prêts pour le RGPD, non seulement vous mettez en place des mesures concrètes et réalistes pour qu'ils soient en conformité, mais vous pouvez également identifier de nouvelles opportunités de fournir de nouveaux services à valeur ajoutée qui impliquent d'autant plus votre activité dans leur entreprise.

1. **À quel point vos clients sont-ils prêts pour le RGPD ?**

   Cela aidera vos clients à connaître leur niveau de préparation actuel et à évaluer les aspects du RGPD et de la protection de la vie privée qui ont le plus d'importance dans leur société. Ce n'est pas un exercice où il faut simplement cocher des cases, mais une approche pragmatique et ciblée qui permet de vraiment comprendre à quel point vos clients sont exposés aux risques liés à la protection de la vie privée du RGPD.

2. **Définir une stratégie**

   Il est essentiel de comprendre quels types de données vos clients doivent détenir (et à propos de qui), comment ces données vont être traitées de façon conforme au RGPD, et quels investissements doivent être faits pour déployer cette stratégie. Il faut également prendre en considération 'l'externalisation des données', c'est-à-dire l'utilisation de fournisseurs externes et de logiciels sur le cloud, pour garantir un respect absolu des règles.

3. **Reconnaitre le succès**

   Être en conformité avec le RGPD signifie mettre en place une solution de protection des données appropriée à chaque entreprise en particulier. Avec une approche pragmatique et en établissant un plan réaliste, vous pourrez préparer vos clients à l'entrée en vigueur du RGPD. Cela peut être décomposé en points clé :

- **Gouvernance : Comprendre quelles données personnelles vos clients détiennent, et comment ils comptent les gérer.**
- **Droits individuels : Savoir ce qu'un individu peut réclamer et quels sont ses droits. Définissez vos procédures en conséquence pour gérer ce genre de requêtes.**
- **Signaler les failles de sécurité : Mettez en place des procédures de gestion des incidents efficaces afin d'être en conformité avec les exigences du RGPD, qui réclame que les incidents soient rapportés à l'agence de réglementation sous 72 heures.**
- **Le recours à des tiers : Les responsables du traitement des données doivent comprendre comment leur chaîne d'approvisionnement gère les données. Des contrats comportant les clauses nécessaires, les périodes de rétention et les systèmes de vérifications doivent être en place à temps pour l'entrée en vigueur du RGPD.**
- **Formation : Identifiez le niveau de formation nécessaire pour les différentes personnes de votre entreprise afin qu'elles comprennent mieux les obligations du RGPD. Les fonctions « à haut risque », comme les RH ou le marketing, peuvent réclamer un niveau plus élevé de formation et de support.**

4. **Faites-en une pratique habituelle**

   La conformité au RGPD implique bien plus que de simplement être prêt pour sa mise en application le 26 mai 2018. À l'avenir, vos clients devront prouver que la façon qu'ils ont de collecter, utiliser, conserver, dévoiler et détruire des données personnelles est conforme aux obligations du RGPD. Cela représente une transformation profonde des processus et méthodes de travail actuels qui doit être prolongée afin de refléter le principe de responsabilité inclus dans le RGPD. Cela implique que :

- **Les entreprises doivent avoir un cadre de gestion du risque documenté et clair**
- **Les données personnelles doivent être gardées à jour et être accessibles afin de répondre aux demandes des sujets des données**
- **Les rôles et responsabilités en matière de protection des données personnelles doivent être clairement définis, et doivent être vérifiés en permanence**
- **Des politiques, processus et procédures bien gérés et adaptés doivent être en place**
- **Une transparence totale doit être mise en place concernant l'utilisation des données que vous fournissez par des tiers.**

En sécurité avec Sage

L'engagement de Sage pour le RGPD

Depuis 30 ans, Sage s'engage aux cotés des comptables et experts-comptables et les aide à se mettre en conformité avec les réglementations clé ; aujourd'hui, il en est de même avec le RGPD. Nos experts sont là pour vous aider et vous apporter leur soutien pratique, impartial et concerté et vous conseiller afin de vous aider à comprendre l'impact de la conformité au RGPD sur votre activité et vos clients. Nous nous engageons à vous apporter les connaissances et compétences nécessaires à votre activité et vos clients pour vous préparer à l'entrée en vigueur du RGPD.

Nous publions des présentations de nos produits qui expliquent comment notre gamme de logiciels est prête pour le RGPD afin de vous aider à vous mettre en conformité. En outre, notre programme de formations est conçu pour vous aider, vous et vos clients, à relever le défi de la préparation au RGDP. Il comprend un ensemble de formations conçues spécialement pour les experts-comptables, y compris des sessions d'entrainements avec vos clients.

Grâce à des nouvelles méthodes de travail, vous allez non seulement vous préparer à la mise en place du RGPD, mais également bénéficier de méthodes plus efficaces grâce à une gestion intégrée des données personnelles, et ainsi mieux conseiller vos clients sur les réglementations clé qui affectent leurs activités.

Sage University - des options de formations sur le RGPD

Chez Sage, nous nous engageons à vous aider à passer un nouveau cap et à combler des besoins complexes en matière de conformité aux règlements.

Nous investissons dans notre technologie afin de vous offrir des solutions qui vous aident, vous et vos clients, à vous préparer à cette modification majeure de la législation qu'est le RGPD. Notre équipe chargée des formations, via la plateforme Sage University, propose éducation et formation, ainsi que des ressources commerciales rassemblées au même endroit.

Pour en savoir plus sur nos services de formations et les options gratuites et payantes, visitez le site sage.com/GDPR. Vous pouvez également contacter votre interlocuteur commercial Sage pour en savoir plus sur nos offres de formations et d'entraînement.

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.

Avec Sage comme partenaire, vous avez le meilleur pour votre cabinet et pour vos clients, à chaque étape.

Pour en savoir plus, visitez
www.sage.com/fr-fr/informations-legales/rgpd/

©2018 The Sage Group plc, ou ses partenaires. Tous droits réservés. Les marques, les logos et les noms des produits et services Sage mentionnés sont les marques appartenant à The Sage Group plc, ou à ses partenaires. Toutes les autres marques sont la propriété de leurs titulaires respectifs.