DocuWare

White Paper
RGPD

Clause de non-responsabilité

Le plus grand soin a été apporté à la rédaction de ce document et les informations qu'il contient proviennent de sources fiables. Cependant, nous ne pouvons en aucun cas être tenu responsables de la correction, l'exhaustivité ou l'actualité des dites informations. Aucune réclamation ne peut découler de l'utilisation des informations fournies dans le présent document. DocuWare GmbH se réserve le droit de modifier les informations contenues dans ce document à tout moment, sans préavis.

DocuWare GmbH
Therese-Giehse-Platz 2
82110 Germering
www.docuware.com (http://www.docuware.com)

DocuWare

Sommaire

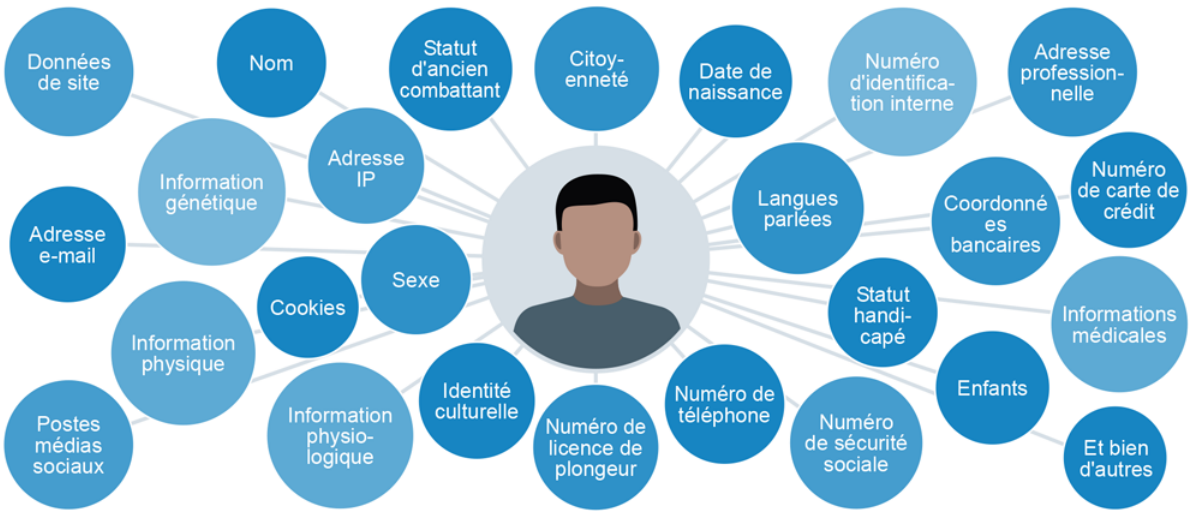
1 Le respect du RGPD de l'UE est une nécessité absolue

Le RGPD, ou Règlement général sur la protection des données, présente une nouvelle série de règles et normes européennes, portant sur la protection de la vie privée et la gouvernance des données. Il ne s'applique pas seulement aux sociétés européennes, mais à toute société exploitant ses activités en Europe ou faisant affaires avec des clients européens. Le règlement exige le consentement éclairé des clients et leur confère de nouveaux pouvoirs en termes de portabilité, leur permettant de contrôler le transfert des informations les concernant. Il établit des sanctions sévères en cas de non-conformité. Ce règlement prend effet à compter de mai 2018.

On pourrait être tenté de penser que rien ne change vraiment avec le RGPD. Après tout, l'Europe a, depuis 1995, mis en place des règlements sur la gouvernance et la protection des données. Mais le RGPD constitue une série de principes jouissant de la plus haute priorité et exigeant l'attention de toutes les entreprises.

Les six principes du RGPD

Le cœur même du RGPD concerne la protection des données personnelles ou des informations d'identification personnelle (IIP). Les données personnelles peuvent consister en des informations de tout genre permettant à une personne d'identifier directement ou indirectement une autre personne physique. Ces données incluent des informations telles que les noms, adresses e-mail, les publications sur les médias sociaux, les informations physiques, physiologiques, génétiques ou médicales, les lieux, les coordonnées bancaires, les adresses IP, les cookies et l'identité culturelle.



Cette protection est établie en six principes. Ces données doivent être :

1 traitées en toute légalité, de manière loyale et transparente ;

2 recueillies à des fins spécifiées, explicites et légitimes ;

3 appropriées, pertinentes et limitées au strict nécessaire ;

4 précises et, si nécessaire, mises à jour ;

5 conservées uniquement tant qu'elles sont nécessaires ;

6 traitées de manière à garantir leur sécurité.

Vous devez non seulement respecter les six principes généraux du RGPD, mais devez également démontrer votre conformité via la documentation et/ou les procédures opérationnelles standard (POS) sur la protection des données.

Informations importantes à savoir

1 **Le RGPD est un Règlement de l'UE qui prime sur tous les autres :** Contrairement à la directive précédente de l'UE sur la confidentialité des données, le nouveau RGPD est un règlement de l'UE. Ce qui signifie qu'il prendra immédiatement effet le 25 mai 2018 à l'issue d'une période de transition de deux ans et que contrairement à une directive, il ne nécessite pas l'adoption d'une loi habilitante par des gouvernements nationaux. À l'instar de tout règlement de l'UE, le RGPD s'assimile à une loi européenne. Il prévaut sur les lois nationales et toutes les directives précédentes de l'UE.

2 **Sanctions élevées :** Les sanctions imposées en cas de non-respect sont importantes. Des amendes peuvent être appliquées à hauteur de 20 millions d'euros ou 4 % du total du chiffre d'affaires annuel mondial du précédent exercice financier, selon le montant le plus élevé (Article 83 : Conditions générales relatives à l'imposition d'amendes administratives)

3 **Consentement éclairé du client :** Un consentement valide doit être explicitement donné pour le recueil des données et les fins auxquelles elles sont utilisées (Article 7 : défini à l'Article 4). Par ailleurs, les responsables du traitement des données doivent pouvoir démontrer le « consentement » (option positive) et celui-ci doit pouvoir être retiré.

4 **Respect en dehors de l'UE :** Les anciennes clauses de sauvegarde applicables aux sociétés non européennes n'ont plus cours. Les sociétés non européennes recouraient aux dispositions d'exonération pour se conformer au règlement d'origine sur la protection des données. En juillet 2000, la Commission européenne (CE) a décidé que les sociétés américaines se conformant aux principes et déclarant satisfaire aux conditions de l'UE pouvaient transférer des données de l'UE vers les États-Unis. Mais, les Principes internationaux de la Sphère de sécurité, relatifs à la protection de la vie privée, ont été infirmés le 24 octobre 2015 par la Cour de justice de l'Union européenne, lorsqu'un client s'est plaint de l'insuffisance de protection de ses données publiées sur Facebook.

5 **Les données personnelles peuvent inclure tout type de données :** La gestion d'informations et de documents non structurés est essentielle au respect de la conformité. Selon la Commission européenne, les « données personnelles consistent en tout type d'informations relatives à une personne, qu'elles aient trait à sa vie privée, professionnelle ou publique ». La Commission indique « qu'il peut s'agir de tout type de renseignements incluant un nom, l'adresse du domicile, une photo, une adresse e-mail, des coordonnées bancaires, des publications sur les réseaux sociaux, des informations médicales ou l'adresse IP d'un ordinateur ». Les sociétés doivent pouvoir identifier **les lieux ou documents** contenant des informations d'identification personnelle et pouvoir fournir au client, un index de ces données d'identification personnelle, si celui-ci en fait la demande : condition qu'il est impossible de remplir en l'absence de système de gestion du contenu.

6 **Les documents au format papier sont inclus :** Le RGPD s'applique au traitement des données personnelles par voie totalement ou partiellement automatisée. Fait encore plus important : Il s'applique également au traitement de données personnelles par des moyens autres que des procédés automatisés, si ces informations font partie ou sont

destinées à faire partie d'un système de classement. (Article 2 : Champ d'application concret)

7 **Chaînes de responsabilité étendues :** Si des informations d'identification personnelle sont stockées ou gérées en votre nom, par un prestataire de services cloud ou un prestataire externe de traitement des documents, vous continuez à assumer la responsabilité des pratiques de gouvernance des données adoptées par vos prestataires externes.

Connaître vos fonctions : responsable et/ou sous-traitant en charge du traitement des données

Dans le cadre du RGPD, vous devez avoir entendu parler de cinq termes ou rôles : la personne concernée, le responsable du traitement des données, le sous-traitant du traitement des données, le délégué à la protection des données et l'autorité en charge de la protection des données.

- La **personne concernée** est une personne physique. Il peut s'agir d'un client ou d'un employé d'une société, d'un utilisateur de la plateforme de médias sociaux ou d'une autre personne. Le rôle de la personne concernée peut être comparé au concept (ou terme) juridique du propriétaire de données, dans ce cas. Tout citoyen est concerné : « Les principes et les règles applicables à la protection des personnes physiques, quant au traitement de leurs données personnelles, doivent, indépendamment de leur nationalité ou de leur lieu de résidence, respecter leurs droits et libertés fondamentaux et particulièrement leur droit à la protection des données personnelles ». La personne concernée bénéficie de plusieurs droits lui permettant d'obtenir des renseignements sur le type d'informations d'identification personnelle qui sont stockées et traitées, de demander leur correction voire leur suppression ainsi que leur transfert en faveur d'une autre société. Le rôle de la personne concernée peut être comparé au concept (ou terme) juridique du propriétaire de données, dans ce cas.
- Un **responsable du traitement des données** « signifie la personne physique ou morale, l'autorité publique, l'organisme ou toute autre organisation, qui seul ou en association avec des tiers, détermine les fins et moyens de traitement des données personnelles ; lorsque les fins et moyens de ce genre de traitement sont déterminés par la législation de l'Union européenne ou d'un État membre, le responsable du traitement ou les critères spécifiques entourant sa désignation peuvent être prévus par la législation de l'Union européenne ou de l'État membre ». Le rôle du responsable du traitement des données peut être comparé au concept (ou terme) juridique du possesseur.
- Un **sous-traitant en charge du traitement des données** est une « personne physique ou morale, une autorité publique, un organisme ou toute autre organisation qui traite les données personnelles au nom du responsable du traitement des données ».

Votre société peut être le responsable et/ou le sous-traitant du traitement des données. Vos clients, prospects et fournisseurs peuvent également être des responsables ou sous-traitants du traitement des données. De même, vos clients, prospects, employés et travailleurs indépendants sont tous des personnes concernées, à l'instar des groupes semblables de vos partenaires.

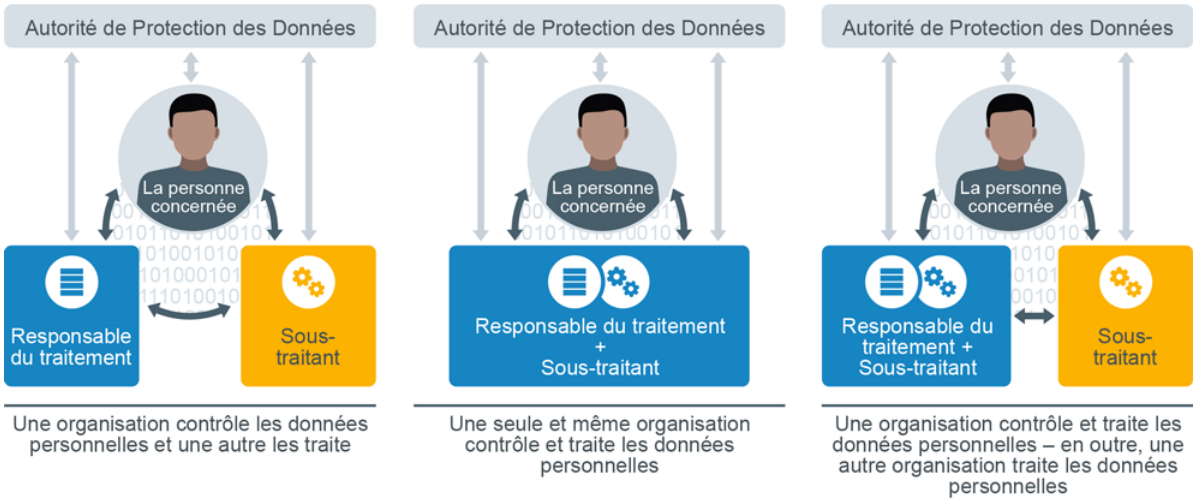
Article 4 : Définitions

Dès le début, les responsables et sous-traitants du traitement des données doivent intégrer un outil de sécurité aux produits et procédés. Si ce n'est déjà fait, les responsables et sous-traitants du traitement des données doivent désigner un **délégué à la protection des données** (DPD) qui sera également responsable si vous :

- traitez les informations d'identification personnelle de plus de 5 000 personnes concernées par an ;
- êtes une organisation ou un organisme gouvernemental ;
- traitez principalement des catégories spéciales de données ;
- effectuez régulièrement une observation à grande échelle.

Article 37 : Désignation du délégué à la protection des données http://www.privacy-regulation.eu/fr/37.htm

Chaque État membre de l'UE prévoit une ou plusieurs **autorités indépendantes chargées de la protection des données** (APD) responsables du contrôle du secteur privé.



Qui peut se plaindre et à qui doit-il s'adresser ?

Dans le cadre du RGPD, non seulement une personne peut déposer plainte, mais elle peut également mandater une organisation à but non lucratif, une association de protection des consommateurs, par exemple, afin qu'elle le fasse en son nom.

Article 80 : Représentation des personnes concernées

Un procès est entamé devant les tribunaux de l'État membre de l'UE, où le responsable ou sous-traitant du traitement des données dispose d'un établissement (Principe du guichet unique). Il peut également s'agir des tribunaux de l'État membre où le demandeur ou la personne concernée a élu sa résidence habituelle.

Article 79 : Droit à un recours judiciaire effectif à l'encontre d'un responsable ou d'un sous-traitant du traitement des données

2 Comment DocuWare peut vous aider à respecter le RGPD

Un e-mail, un fichier, un papier, une note ou un document contenant des informations d'identification personnelle, constitue des données personnelles. Ce qui signifie qu'ils doivent être stockés, gérés, protégés et contrôlés conformément au RGPD.

Si le RGPD est assez clair sur le niveau de protection requis pour les données personnelles, il n'énonce pas précisément les procédés ou technologies auxquels les sociétés doivent recourir pour assurer cette protection. En fait, il est peu probable qu'un seul et même système puisse satisfaire chaque facette de ce règlement. Le respect de ce règlement exigera un effort coordonné associant technologie et politiques.

Le système de gestion des documents constitue une technologie importante, qui non seulement numérise les registres au format papier tout en profitant des métadonnées pour appliquer la sécurité et la gouvernance requises pour protéger les données des clients.

Fort de son approche axée sur le contrôle, DocuWare soutient directement vos projets de conformité avec le RGPD. Par exemple, dans DocuWare, des classeurs peuvent être mis en place afin d'éviter le téléchargement, le transfert ou l'impression des documents. Cette procédure ne nécessite aucune programmation, aucun codage ni long processus de mise en œuvre : il s'agit d'une fonction de base.

2.1 Trouvez et accédez aux données personnelles

Si une personne vous demande quel type de données personnelles la concernant est traité dans votre société, vous devez d'abord **localiser les données personnelles**. Toutefois, dans la mesure où le RGPD s'applique également aux registres **papier** stockés par une entreprise, cela peut être plus facile à dire qu'à faire si vous gérez encore les procédures au format papier.

Comment DocuWare peut-il favoriser votre conformité

Grâce à DocuWare, tous vos documents sont numérisés et stockés dans un système sécurisé, de sorte que vous puissiez facilement **trouver et accéder à toutes les données personnelles** figurant dans vos documents. Il peut s'agir d'e-mails, de contrats, de factures, etc. DocuWare peut automatiser la procédure de stockage, de découverte, de localisation, d'exportation et de suppression des informations d'identification personnelle.

Cette procédure ne dépend donc plus des personnes. Mais s'applique à des politiques d'entreprise de gouvernance des données. L'approche automatisée de protection des informations d'identification personnelle confère ordre, cohérence et efficacité à vos procédés d'entreprise et vous permet de respecter plus rapidement et facilement les conditions du RGPD. L'équipe de DocuWare vous aide à établir une stratégie de numérisation pour vos registres papier.

Les métadonnées jouent un rôle essentiel dans le respect du RGPD puisqu'elles permettent de correctement classer, hiérarchiser et décrire les informations d'identification personnelle conformément aux conditions du règlement. Un exemple de base consisterait à faire de simples recherches par type de documents (contrats, factures, correspondance) qui selon vous contiennent des informations d'identification personnelle.

DocuWare Intelligent Indexing utilise l'apprentissage automatique et l'intelligence artificielle (IA) pour automatiser cette procédure de classement, ce qui garantit la conformité tout en soulageant votre équipe d'une saisie de données longue et compliquée.

Lorsqu'un document est stocké, DocuWare peut automatiquement entamer d'autres actions afin de garantir le traitement et la gestion appropriés des informations. Il peut notamment :

- crypter tous les fichiers et objets qui contiennent des informations d'identification personnelle ;
- appliquer un contrôle des accès et gérer les autorisations, permettant de garantir que seuls les utilisateurs habilités puissent accéder aux informations d'identification personnelle. Par exemple, les représentants du service client, contrairement aux équipes marketing, peuvent visualiser les commandes des clients ;
- appliquer des règles relatives à la conservation et à la suppression, de façon à garantir que les données ne sont pas conservées plus longtemps que nécessaire ;
- éviter que des documents contenant des informations d'identification personnelle ne soient délibérément ou involontairement envoyés par e-mail ou transférés de toute autre manière en dehors de l'entreprise ;
- assurer le suivi des modifications apportées aux documents contenant des informations d'identification personnelle, afin d'indiquer les changements apportés, l'identité de la personne ayant effectué les changements et la date à laquelle ces changements ont été apportés ;
- fournir une piste de vérification afin de prouver que seuls les employés habilités ont eu accès aux informations d'identification personnelle des clients.

Automatiser cette approche de protection des informations d'identification personnelle confère ordre, cohérence et efficacité à la tâche, tout en appliquant des politiques de gouvernance des données au niveau de l'entreprise.

2.2 Obtenez la possibilité d'exporter, de corriger et de supprimer les données personnelles

Si l'on vous pose des questions sur les informations d'identification personnelle, vous devez pouvoir **exporter** les données personnelles afin de les montrer au demandeur. Cette condition peut également permettre à cette personne de transférer ses données sous un « format couramment utilisé et lisible par machine » à un autre distributeur ou prestataire de services.

Vous devez gratuitement fournir un exemplaire des données personnelles faisant l'objet d'un traitement, dès la première demande. Par ailleurs, vous devez le faire dans un délai de 30 jours.

Si votre société détient des informations personnelles inexactes, vous devez immédiatement les **corriger** sur demande. Si une personne tient à ce que ses données soient **supprimées**, vous devez également y consentir, en vertu du droit à l'oubli. Vous pouvez seulement refuser de supprimer des données pour respecter une obligation juridique, servir les intérêts publics ou répondre à des réclamations juridiques.

Comment DocuWare peut-il favoriser votre conformité

Toute demande d'exportation, de correction ou de suppression de données personnelles peut être stockée dans DocuWare et peut automatiquement déclencher un processus de travail approprié, spécialement conçu pour exporter, corriger ou supprimer les informations d'identification personnelle. Les tâches du processus de travail peuvent être automatiquement affectées au délégué à la protection des données (DPD) qui décidera si cette demande est ou non justifiée.

Dans le cadre du Module de Demande, la portabilité des données représente une fonction originale de DocuWare. Vous pouvez facilement **exporter et transférer** toutes les informations d'identification personnelle.

Article 20 : Droit à la portabilité des données

La visionneuse DocuWare garantit que tous les changements de document apportés dans la visionneuse sont stockés en superposition du document. Vous pouvez donc exporter une facture contenant les informations d'identification personnelle d'un client sans émettre le timbre ou les informations d'identification personnelle de l'un de vos employés.

Les tâches du processus de travail peuvent être affectées aux délégués à la protection des données (DPD). Ils mettront alors eux-mêmes à jour les données figurant dans les différents systèmes ou les affecteront à des collègues compétents. Le DPD peut facilement **accéder à tous les registres** sur les personnes concernées et les cocher en vue de leur suppression. Un processus de travail DocuWare enclenche automatiquement des actions lorsque le DPD a confirmé le fait que la demande était justifiée.

Pour **corriger** toutes les données concernées, les métadonnées stockées dans DocuWare peuvent être mises à jour de manière automatique ou semi-automatique dans le cadre de ces procédés. Ce qui garantit la cohérence entre les systèmes et renforce votre respect du RGPD.

Si nécessaire, DocuWare peut **supprimer à la fois les documents et les métadonnées**. DocuWare peut également ouvrir des applications tierces, ce qui simplifie ces tâches. DocuWare peut automatiquement informer la personne concernée du fait que les données sont destinées à être supprimées et établir un calendrier de destruction.

DocuWare conserve **l'historique** complet des demandes de rectification des données. Lorsque la demande d'une personne n'est pas justifiée, DocuWare peut aider le DPD à envoyer une réponse automatique au demandeur assortie d'une explication **sur le fait que la demande n'est pas justifiée** et que la société ne traitera plus ses données. Les données de la demande seront conservées pendant une période nécessaire avant d'être automatiquement détruites.

2.3 Veillez à ce que les données personnelles soient protégées et ne fassent pas l'objet d'un traitement ultérieur

Sur demande, votre société doit pouvoir **exclure les données personnelles de ses futures activités de traitement**, que ce soit de manière temporaire ou permanente. Les conditions incluent la précision contestée des données, un traitement illégal et le souhait de la personne concernée d'être exclue des activités de traitement, sans que ses données personnelles ne soient pour autant supprimées pour diverses raisons juridiques et historiques.

Article 18 : Droit à la limitation du traitement

Comment DocuWare peut-il favoriser votre conformité

DocuWare applique les règles relatives à la conservation et à la suppression, de sorte à garantir que les données ne sont pas conservées plus longtemps que nécessaire. En établissant des programmes automatiques de rétention, vous pouvez facilement éviter que des documents contenant des informations d'identification personnelle ne soient délibérément ou involontairement envoyés par e-mail ou transférés de toute autre manière en dehors de l'entreprise. La mise en place de ce programme ne nécessite aucun codage ni aucune programmation. Cela s'inscrit dans la configuration de base, mise à la disposition des gestionnaires ou DPD.

Par ailleurs, toute modification apportée aux documents contenant des informations d'identification personnelle fait l'objet d'un suivi afin d'indiquer les changements apportés, l'identité de la personne ayant effectué les changements et la date à laquelle ces changements ont été apportés. Grâce à une gestion flexible et sécurisée des droits, seuls les employés habilités peuvent avoir accès aux informations d'identification personnelle des clients ; pour prouver l'absence de tout accès non autorisé, le système procure une piste de vérification.

DocuWare prend donc d'importantes décisions sur le mode de gestion des informations d'identification personnelle, déchargeant ainsi les employés individuels et applique des politiques de gouvernance des données au niveau de l'entreprise.

3 Définir une stratégie de conformité au niveau de la société

Le recours à un système de gestion des documents, tel que DocuWare, constitue une avancée importante en faveur du respect du RGPD. Mais, votre société utilise également d'autres logiciels qui traitent des données personnelles, telles qu'un système de CRM, un système marketing, un ERP et d'autres outils.

Pour gérer des données personnelles sur tous les systèmes, vous devez définir une stratégie cohérente. Dans votre système de CRM, par exemple, vous devez également être en mesure de trouver, accéder, corriger, exporter, protéger et supprimer des données personnelles ainsi que de tenir un registre de ces activités de traitement.

Tenez vos registres à jour.

Que ce soit avec votre système de gestion des documents, votre système de CRM ou votre ERP, si vous intervenez en qualité de responsable du traitement des données, votre DPD garantit la conformité et doit donc tenir un registre des informations suivantes :

- votre nom et vos coordonnées et si nécessaire, l'identité des co-responsables du traitement, des représentants et délégués à la protection des données ;
- l'objet du traitement ;
- une description des catégories de personnes concernées et de données personnelles ;
- les catégories de destinataires, incluant ceux se trouvant dans des pays tiers ou les organisations internationales ;
- les renseignements sur les transferts de données personnelles à destination de pays tiers (si nécessaire) ;
- les périodes de conservation des différentes catégories de données personnelles (si possible) ; et
- une description générale des mesures de sécurité utilisées (si possible).

Si vous faites appel à un sous-traitant chargé du traitement des données, vous devez contractuellement vous assurer que CELUI-CI tient un registre de toutes les catégories d'activités de traitement au nom du responsable du traitement des données.

Article 30 : Registres des activités de traitement

Et ne pas oublier : Procéder à une évaluation des risques et à une analyse d'impact relative à la protection des données conformément à l'article 35. Un guide Bitkom vous aide à démarrer.

Complément d'information

RGPD accompagné d'une table des matières et d'une recherche rapide

Ebook « Confidentialité et sécurité des informations» par l'association industrielle AIIM

Prêt pour le RGPD? par Maître Rolf Becker, Cologne

Téléchargement du RGPD dans toutes les langues de l'UE (la version anglaise prévaut d'un point de vue juridique)