TDL | Trust in Digital Life

RGPD pour les PMEs

Orientations pour les petites et moyennes entreprises sur la manière d'aborder la conformité à la protection des données

Une publication du groupe de travail TDL
Décembre 2018
Version 1.0

Contenu

Introduction 3

Ce que vous voulez savoir 4

Ce que vous devrez faire 5

Protection des données par conception 6

Liste de contrôle 7

Conclusion 8

Un instantané RGPD 9

Introduction

Le 25 mai 2018, le règlement général sur la protection des données (RGPD) est entré en vigueur. Il s'agit d'une refonte majeure de la législation existante en matière de protection des données, qui a été mise en place à une époque où très peu de personnes utilisaient Internet. Enfin, le RGPD consacre dans la loi le droit inaliénable des personnes à ce que toutes les données qui les concernent soient protégées et gérées de manière adéquate, avec des sanctions sévères et des amendes pour les entreprises non conformes.

Si votre entreprise figure parmi les milliers de personnes dans l'Union européenne et au-delà qui ne connaissent pas le RGPD ou les conséquences de sa non-conformité, vous devriez lire la suite. Notre intention n'est pas de plonger dans les 99 articles du règlement, mais de fournir un aperçu des principes directeurs qui les sous-tendent et de la manière dont un cauchemar de conformité potentiel peut être transformé en un avantage et un avantage commerciaux.

De nouvelles mesures législatives, telles que le RGPD, sont sur le point d'avoir un impact majeur sur les entreprises qui détiennent des données sur les citoyens de l'UE. Les lourdes amendes pour non-conformité ou dépassant 20 millions d'euros ou 4% du chiffre d'affaires global ne constituent pas, comme on pourrait le penser au départ, des formalités administratives ni des coûts commerciaux sans finalité commerciale. Au contraire, l'objectif de la nouvelle législation est d'accroître la confiance des clients dans les services numériques et d'accélérer ainsi l'adoption de la technologie, avec toutes les efficiences et tous les avantages économiques qui en découlent. Il harmonise également les lois sur la gestion des données pour les entreprises de toute l'Europe, tout en réduisant les coûts juridiques à moyen terme et en facilitant les opportunités de participation des clients au niveau pan-européen.

Avant l'introduction du RGPD fin mai 2018, les citoyens de l'Union européenne ont été condamnés à recevoir des courriels et autres communications de détaillants, d'institutions financières, d'agences de voyages en ligne, de fournisseurs de services, d'agences gouvernementales locales et bien d'autres. Ils cherchaient tous à s'assurer que les clients passés et présents ont consenti au stockage continu de leurs informations personnelles dans des bases de données d'entreprise et des systèmes CRM et à leur utilisation future à des fins clairement identifiées. Derrière cette activité, il y a un énorme volume de travail administratif à réviser, analyser, valider et nettoyer systématiquement toutes les données personnelles accumulées afin de s'assurer que les informations enregistrées étaient légalement.

En conséquence, la plupart des citoyens ont au moins pris conscience de l'existence du nouveau règlement, même s'ils ne connaissaient pas parfaitement les détails. On peut en dire autant de la plupart des entreprises et des organisations, grandes ou petites, à la différence que bien que les grandes entreprises disposent de beaucoup plus de systèmes de stockage de données, elles disposent généralement de beaucoup plus de ressources pour comprendre, interpréter et gérer ce qui doit être fait que de petites entreprises. -à-moyennes entreprises.

Malgré l'apparente fatigue générale générée par le RGPD depuis mai dernier, le règlement n'a pas disparu et est surveillé de près par les autorités nationales chargées de la protection des données dans chacun des États membres de l'UE, ainsi que par l'organe de surveillance principal basé à Bruxelles. Bien que les PME puissent faire preuve d'un peu de clémence, compte tenu des difficultés qu'elles rencontrent pour se mettre en conformité, toute période de lune de miel devra inévitablement prendre fin.

Ce que vous voulez savoir

Sur les 99 articles et 173 considérants (ou définitions juridiques) du RGPD, la plupart sont susceptibles d'interprétation. Si vous n'avez pas le temps et n'êtes pas prêt à les étudier de manière approfondie, il n'est pas raisonnable d'espérer que les PME disposent des ressources nécessaires pour saisir tout ce qui leur est demandé. Alors, qu'est-ce qui va au cœur de la réglementation, les concepts clés pour toute entreprise à connaître et à respecter?

Les principes au cœur du RGPD sont les suivants:

- Donnez plus de pouvoir à vos clients en les informant - avec clarté - des informations que vous avez obtenues et du but pour lequel vous les utiliserez;
- Montrez votre engagement en fournissant aux clients un moyen convivial de donner son consentement et un mécanisme tout aussi simple pour refuser l'utilisation de leurs données, à moins que votre entreprise ne poursuive un objectif clairement légitime.
- Offrir les outils pour contrôler et gérer ces données personnelles au fur et à mesure que leur situation change;
- Informez vos clients qu'ils peuvent contester juridiquement votre entreprise si votre entreprise modifie son objectif ou utilise les données à caractère personnel (sans consentement révisé), ou les perd en raison de soins insuffisants.

Notification de violation de données

Si vous êtes assez malheureux pour avoir subi une violation de données, vous êtes maintenant obligé d'avertir les autorités ainsi que toutes les personnes qui, selon vous, ont été touchées.

Les clients ont le droit de:

- Objet pour que leurs données soient utilisées pour tout marketing
- Divulgation complète de la manière dont leurs données seront traitées
- Objecter au traitement automatique de leurs données à des fins de profilage
- Accès complet aux données
- Exiger que leurs données soient rectifiées si elles sont inexactes
- Exigez que vous effaciez leurs données
- Obtenir une copie de leurs données sous une forme qu'ils peuvent apporter à votre concurrent (connue sous le nom de «portabilité des données»)

Bonnes nouvelles!

Il n'existe pas beaucoup d'exemptions pour les PME; il est donc important de souligner celle qui réduit le fardeau: les PME sont dispensées de l'enregistrement des opérations de traitement (inventaire).

Ce que vous devrez faire

Réalisez un audit de données

Identifiez toutes les données personnelles dont vous êtes responsable et localisez-les. Vous pourriez être surpris à quel point vous tenez.

Identifiez le traitement des données

Clarifiez la manière dont vous traitez les données à caractère personnel et déterminez si ce traitement est conforme à vos intérêts commerciaux légitimes.

- ***Obtenez le consentement:** si vous avez besoin de ces données à des fins commerciales, vous devrez valider votre consentement explicite pour l'accès à ces données et leur traitement..*
- ***Effacez et retirez**: si ce n'est pas le cas, envisagez de supprimer les données et de supprimer ces processus.*

Vérifiez la conformité du fournisseur

Si vous faites appel à des tiers pour vous aider à traiter les données, et vous faites presque certainement, auditez ces fournisseurs et demandez-leur de confirmer leur conformité au GDPR. Vous devrez peut-être même réviser vos contrats de service avec eux afin de vous indemniser de manière appropriée. À leur tour, ils exigeront sans aucun doute la confirmation de votre consentement vérifiable aux fins d'accès aux données et de traitement.

En bref, la solution simple consiste à faire de votre entreprise la sécurité de la confidentialité et la sécurité des données personnelles de vos clients. Intégrez la mentalité de «client maître» dans votre traitement numérique et en ligne et vous ne vous tromperez pas. De nombreuses personnes hésitent de plus en plus à transmettre des informations personnelles sur Internet. Les entreprises peuvent prendre des mesures simples pour minimiser ces risques en adaptant leurs pratiques de travail afin de présenter un avantage en matière de confidentialité aux clients.

Restez simple, mince et méchant

Un principe clé du RPGD est la minimisation des données, ce qui signifie non seulement qu'il ne faut pas détenir de données personnelles dont vous n'avez pas strictement besoin, mais également que vous ne les conservez pas plus longtemps que nécessaire. Une violation a des conséquences pour votre client et, si vous n'avez pas besoin de conserver les données qui ont été violées, attendez-vous à une augmentation des amendes. Les entreprises innovantes trouveront des moyens de fournir un service avec moins de données et potentiellement différencieront leur offre de prospects, en particulier pour les données juridiquement sensibles ou considérées comme sensibles par les prospects de votre secteur.

Pas de repas gratuits

C'est étonnant de voir combien de sociétés négligent le logiciel tiers (surtout gratuit) qu'elles utilisent pour créer des sites Web et recherchent généralement les fournisseurs de services Internet ou les systèmes CRM les moins chers. Bien que les systèmes de gestion de contenu (CMS) les plus répandus soient sécurisés de manière fiable, de nombreux plug-ins associés peuvent ne pas l'être. Les logiciels «gratuits» sont rarement sans piège - vous pouvez être assez sûr que le prix est extrait dans vos données client - alors vérifiez, car vous êtes maintenant responsable! Les services bon marché peuvent également utiliser les mêmes techniques, le même prix commercial pour votre entreprise ou les données de vos clients.

Processus d'affaires

La plupart de ce qui précède concerne en réalité les processus métier - non pas, comme le pensent la plupart des entreprises, une responsabilité des TI qui ont un rôle à jouer dans la validation des fournisseurs, mais dans le contexte du RGPD, son rôle principal est d'éviter les violations. Le service informatique sera également responsable de la détection et du signalement des violations (avez-vous des outils pour cela? Beaucoup n'en ont pas). Ce rapport est transmis au responsable du traitement de données désigné par la société, qui doit ensuite décider s'il doit être signalé à l'autorité de surveillance nationale pour la protection des données. Un regroupement d'infractions mineures au fil du temps peut indiquer une défaillance systémique à résoudre. L'autorité de surveillance attend un journal de toutes les infractions mineures internes et, si elles indiquent un problème systémique de ce type, elles s'attendent à ce qu'il soit résolu, en particulier si cela conduit ultérieurement à une infraction plus grave.

Protection des données par conception

Sites Web destinés au public.

Google Analytics est installé sur de nombreux sites Web sans trop réfléchir aux données collectées sur les visiteurs.
Si vous n'avez jamais pris une seule décision basée sur l'analyse Web, vous devriez envisager de l'éliminer. Et pendant que vous y êtes, examinez la politique de confidentialité de votre site Web et la politique en matière de cookies. Déterminez si les logiciels d'analyse et de suivi (y compris les boutons de réseaux sociaux) que vous utilisez valent la peine d'être rendus conformes à la norme RGPD.

En ce qui concerne la confidentialité des utilisateurs, le RGPD a tenté de légaliser les sept principes de la protection de la vie privée dès la conception qui s'appliquent non seulement au développement de logiciels, mais également aux processus et procédures de l'entreprise. En d'autres termes, chaque PME doit avoir un processus pour traiter les données personnelles.

Examiner les processus de votre entreprise par rapport à ces principes peut vous aider à comprendre à quel point vous êtes loin d'avoir la bonne culture de leadership pour atténuer les risques et maximiser les opportunités commerciales. Si vous suivez ces principes à la lettre, vous constaterez peut-être que le consentement est peu nécessaire et vos services disposeront de peu de paramètres de confidentialité, voire aucun. Toute confidentialité est contextuelle - vous comprenez quelles données vous devez traiter, mais votre client le sait-il? En trouvant des moyens de faire savoir clairement à vos clients les données que vous collectez et ce que vous en faites, vous atténuerez les problèmes de gestion de votre confidentialité.

Les sept principes de la protection de la vie privée dès la conception sont les suivants:

- Proactif non réactif: préventif, pas correctif
  Adoptez une approche proactive de la protection des données et anticipez les problèmes et les risques de confidentialité avant qu'ils ne surviennent, au lieu d'attendre qu'il soit trop tard.
- Confidentialité comme paramètre par défaut
  Concevoir des systèmes, des services et des processus pour protéger automatiquement les données personnelles. Intégrez la confidentialité dans toutes les pratiques commerciales de votre entreprise et les clients apprendront à croire que leurs données sont correctement protégées.
- Confidentialité intégrée à la conception
  Intégrez la protection des données à la conception de vos systèmes, services et processus, en intégrant la confidentialité dans les fonctionnalités essentielles.
- Fonctionnalité complète - somme positive et non nulle
  Assurez-vous que tous les systèmes sont compatibles avec la confidentialité et la sécurité, et qu'il n'y a pas de compromis inutiles.
- Sécurité de bout en bout - protection du cycle de vie complet
  Instanciez des mesures de sécurité strictes garantissant une gestion sécurisée du cycle de vie des données, de leur collecte initiale à leur suppression sécurisée.
- Visibilité et transparence - gardez-le ouvert
  Quelle que soit la pratique commerciale ou la technologie que vous utilisez, vous devez opérer conformément aux lieux et objectifs vérifiables de manière indépendante.
- Respect de la vie privée des utilisateurs - gardez-le centré sur l'utilisateur
  Maintenez l'intérêt des utilisateurs pour la conception des systèmes en offrant de solides valeurs par défaut en matière de confidentialité, des contrôles conviviaux et des notifications appropriées.

Liste de contrôle

La logique commerciale consiste à traiter les données comme un actif commercial quantifiable. L'investissement requis pour protéger ces actifs peut être comparé à l'approche d'une société d'assurance consistant à indemniser la maison et son contenu.

Les PME peuvent aisément s'adapter au nouveau RGPD de différentes manières.

Cette courte liste de contrôle vous aidera à vous conformer au RGPD. Pouvoir répondre «oui» à chaque question ne garantit pas le respect des règles, mais signifie que vous vous dirigez dans la bonne direction.

Données client

- ✓ Avez-vous vraiment besoin de cette information sur un individu? Savez- vous pour quoi vous allez l'utiliser?
- ✓ Les personnes dont vous détenez les informations savent-elles que vous les avez et sont-elles susceptibles de comprendre pourquoi elles seront utilisées?
- ✓ Etes-vous convaincu que les informations sont conservées de manière sécurisée, que ce soit sur papier ou sur ordinateur? Et que dire de votre site Web - est-il sécurisé?
- ✓ Etes-vous sûr que les informations personnelles que vous possédez sont exactes et à jour?
- ✓ Supprimez-vous ou détruisez-vous régulièrement des informations personnelles dès que vous n'en avez plus besoin?
- ✓ L'accès aux informations personnelles est-il limité aux personnes ayant un strict besoin de savoir?

Données du personnel

- ✓ Si vous souhaitez mettre des informations relatives au personnel sur votre site Web, les avez-vous consultées à ce sujet?
- ✓ Si vous souhaitez surveiller le personnel, par exemple en vérifiant son utilisation du courrier électronique, leur avez-vous parlé de cela et expliqué pourquoi?
- ✓ Avez-vous formé mon personnel à ses tâches et responsabilités dans le cadre du RGPD et vous assurez-vous régulièrement qu'il les met en pratique?
- ✓ Si on vous demande de transmettre des informations personnelles, votre personnel et vous-même êtes-vous au clair lorsque le RGPD vous le permet?

Questions de politique

- ✓ Si vous utilisez la vidéosurveillance, est-il couvert par le GDPR? Si oui, affichez-vous des avis expliquant aux gens pourquoi vous utilisez la vidéosurveillance? Les caméras sont-elles au bon endroit ou empiètent-elles sur la vie privée de quiconque?
- ✓ Savez-vous quoi faire si l'un de vos employés ou un client individuel vous demande une copie des informations que vous détenez sur lui?
- ✓ Avez-vous une politique pour traiter les problèmes de protection des données?
- ✓ Devez-vous informer votre bureau du commissaire à l'information national? Si vous l'avez déjà fait, votre notification est-elle à jour ou doit-elle être supprimée ou modifiée?

Conclusion

De nombreuses personnes hésitent de plus en plus à transmettre des informations personnelles sur Internet, même si beaucoup sont inconscientes des risques. Certaines mesures simples peuvent être prises par les entreprises pour minimiser ces risques; Renseignez-vous rapidement et adaptez vos pratiques de travail pour présenter aux clients un avantage en termes de confidentialité..

En savoir plus!

Pour plus de conseils pratiques pour les entreprises sur la manière de mettre en œuvre les exigences RGPD:

- *Le Contrôleur européen de la protection des données (CEPD), l'autorité indépendante de l'UE chargée de la protection des données: https: // edps.europa.eu/data-protection/data-protection/reference-library_fr*
- *Le Comité européen de la protection des données (EDPB): https: //*
- *edpb.europa.eu/our-work-tools/our-documents_en*
- *Bureau du Commissaire à l'information du Royaume-Uni: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/*

Le RGPD a déjà un impact majeur sur les entreprises, grandes et petites, qui détiennent des données sur les citoyens de l'UE. Les lourdes amendes pour non-conformité ou dépassement de 20 millions d'euros ou 4% du chiffre d'affaires global ne constituent pas, comme on pourrait le penser, des formalités administratives à des fins administratives, ni des coûts commerciaux sans objectif commercial.

Prendre la responsabilité

On ne peut s'attendre à ce que les petites entreprises suivent le volume des nouvelles réglementations, mais elles doivent le faire ou risquer leur vie. Chaque homme d'affaires peut comprendre l'importance de disposer d'un ensemble de principes directeurs et il ne s'agit que d'un nouvel ensemble à comprendre et à inculquer à la culture d'entreprise. Donc, pour que tout soit clair: la gestion du nouveau défi est une question de direction, pas une tâche à confier au marketing, aux ventes ou à l'informatique.

Le paradoxe de la vie privée

À mesure que les clients réalisent leurs nouveaux droits, même si seul un petit nombre de personnes commence à interroger vos systèmes et vos processus et à faire part de ses préoccupations aux autorités de surveillance, les coûts pour votre entreprise pourraient augmenter rapidement. Adhérer aux nouvelles lois et chercher des moyens de simplifier les choses pour les clients montre que vous souhaitez que ces nouveaux droits soient facilement accessibles et compréhensibles. Si vous leur donnez le contrôle et la transparence sur les données personnelles que vous détenez et sur ce que vous en faites, la récompense vient en termes de fidélité et de confiance des clients, grâce à laquelle ils offrent davantage de données pour davantage de services.

Une opportunité d'affaires

Pour les entreprises dynamiques et avant-gardistes qui adoptent la nouvelle législation, cela représente une opportunité commerciale. Si cela n'est pas assez attrayant, il convient également de noter que les personnes vont être beaucoup plus puissantes grâce au RPGD avec des droits sur «leurs» données personnelles. Si votre entreprise abuse ou abuse de sa confiance dans la manière dont vous traitez ses données, elle dispose alors de nouveaux droits de poursuite ou même de recours en recours collectif!

En bref, la nouvelle législation est un rééquilibrage des droits et des pouvoirs entre l'individu et le fournisseur à l'ère numérique. Les entreprises qui ne réagissent pas rapidement se retrouveront laissées derrière par des concurrents qui infligent ou imposent des amendes ou des poursuites judiciaires suffisamment lourdes pour détruire leurs entreprises.

Un instantané RGPD

Conscience

Assurez-vous que votre personnel est au courant des modifications apportées au traitement des données par le RGPD.

Informations que vous possédez

Documentez vos données personnelles d'où elles proviennent et avec qui vous les partagez - un audit de données.

Communicant

Passez en revue vos avis de confidentialité actuels et apportez les modifications nécessaires pour vous aligner sur le RGPD.

Droits de client

Vérifiez vos processus et vos procédures pour vous assurer qu'ils couvrent tous les droits des clients, y compris en ce qui concerne la suppression de vos données personnelles ou leur communication dans un format couramment utilisé.

Consentement

Examinez votre demande, enregistrez et gérez votre consentement pour respecter les normes GDPR.

Demandes d'accès client

Mettez à jour vos procédures pour traiter les demandes dans les délais RGPD.

Lois nationales d'application

Plus de la moitié des États membres de l'UE ont promulgué des lois mettant en œuvre le RGPD et, parfois, ces lois contiennent des exigences supplémentaires.

Base légale pour le traitement données personelles

IIdentifiez et documentez le fondement légal de votre traitement des informations personnelles et mettez à jour votre déclaration de confidentialité en conséquence

Les enfants

Déterminez si vous devez mettre en place des systèmes permettant de vérifier l'âge des individus et d'obtenir le consentement de vos parents ou de votre tuteur pour le traitement des données.

Failles de données

Assurez-vous de disposer des procédures adéquates pour détecter, signaler et enquêter sur une violation de données à caractère personnel.

Protection des données par conception

Vérifiez vos processus et procédures pour vous assurer qu'ils couvrent les droits de vos clients, notamment en ce qui concerne la suppression de vos données personnelles ou leur communication dans un format couramment utilisé.

Délégué à la protection des données

Désignez une personne responsable de la conformité à la protection des données et de son rôle dans la structure de gouvernance de votre entreprise.

International

Si vous exercez vos activités dans plusieurs États membres de l'UE, **déterminez** l'autorité de contrôle responsable de la protection des données. Si votre entreprise en ligne utilise des fournisseurs de services non basés dans l'UE, vous devez vous assurer qu'ils sont également conformes au RGPD.

trustindigitallife.eu

Trust In Digital Life Association
avenue Maurice Dekeyser 11 1090 Jette, Bruxelles

office@trustindigitallife.eu
+44 141 5880892

TDL | Trust in Digital Life

La vision de TDL est que la confiance doit devenir une propriété intrinsèque de toute transaction en ligne impliquant des informations personnelles, intégrant des avancées juridiques, commerciales et techniques, prenant en charge des politiques de cybersécurité et intégrant des considérations sociétales afin que les citoyens et les utilisateurs finaux puissent reconnaître des services, transactions et données fiables. et soyez prêt payer pour eux. Des TIC dignes de confiance augmenteront la confiance dans la société moderne, apporteront de nouveaux modes de vie et de travail attrayants et renforceront les valeurs démocratiques et sociales de l'Europe.

L'association a pour mission de fournir à ses membres une plate-forme européenne de développement des entreprises afin de stimuler le développement et l'acceptation par les utilisateurs de TIC fiables mais innovantes et pratiques. Guidé par son agenda de recherche stratégique, TDL agit comme un incubateur pour un portefeuille de projets de sprint visant à valider des concepts technologiques nouveaux et innovants, encourage la collaboration intersectorielle et agrège les résultats dans des recommandations du secteur à l'intention des décideurs et de la Commission européenne.

trustindigitallife.eu

Trust In Digital Life Association
avenue Maurice Dekeyser 11, 1090 Jette, Bruxelles

office@trustindigitallife.eu
T +44 141 5880892

TDL | Trust in Digital Life