Règlement général sur la protection des données (RGPD)

–

Bienvenue chez sceaduparadisier.fr

Un aperçu des nouvelles lois sur la confidentialité et la protection des données qui entreront en vigueur le 25 mai 2018 et quelques bonnes pratiques en matière de conformité RGPD Le RGPD est le changement le plus important dans la régulation de la confidentialité des données depuis des décennies. Les entreprises travaillent à mettre en œuvre des changements radicaux dans leurs systèmes et leurs contrats, et ceux qui fonctionnent sur des plates-formes conformes et respectueuses de la vie privée ont une longueur d'avance. Ce guide vise à aider nos utilisateurs à comprendre les conséquences généralisées du RGPD, l'opportunité qu'il offre d'améliorer les activités de traitement des données et comment devenir et rester conforme au RGPD.

CE GUIDE RGPD EST À TITRE INFORMATIF SEULEMENT. CE N'EST PAS UN AVIS JURIDIQUE. VEUILLEZ CONTACTER VOTRE CONSEILLER JURIDIQUE POUR RECEVOIR DES CONSEILS PERSONNALISÉS SUR LA FAÇON DONT LE RGPD PEUT AVOIR UN IMPACT SUR VOTRE ENTREPRISE.

Qu'est-ce que RGPD?

Le règlement général sur la protection des données («RGPD») est une nouvelle loi européenne sur la protection des données et de la vie privée. Elle exige des garde-fous de confidentialité plus granulaires dans les systèmes d'une organisation, des accords de protection des données plus nuancés et des divulgations plus conviviales et détaillées sur les pratiques de confidentialité et de protection des données d'une organisation.

Le RGPD remplace le cadre juridique actuel de protection des données de l'UE de 1995 (communément appelé «directive sur la protection des données»). La directive sur la protection des données a nécessité une transposition dans la législation nationale des États membres de l'UE, ce qui a conduit à une fragmentation du paysage juridique de la protection des données dans l'UE. Le RGPD est un règlement européen qui a un effet juridique direct dans tous les États membres de l'UE, c'est-à-dire qu'il n'a pas besoin d'être transposé dans la législation nationale des États membres de l'UE pour devenir contraignant. Cela renforcera la cohérence et l'application harmonieuse de la loi dans l'UE. Le RGPD peut s'appliquer aux organisations situées en dehors de l'UE Contrairement à la directive sur la protection des données, le RGPD s'applique à toutes les entreprises opérant à l'échelle mondiale, et pas seulement à celles situées dans l'UE. Dans le cadre du RGPD, les organisations peuvent avoir un champ d'application si (i) l'organisation est établie dans l'UE, ou (ii) l'organisation n'est pas établie dans l'UE mais les activités de traitement de données concernent des individus de l'UE et concernent biens et services à eux ou le suivi de leur comportement.

Le traitement des données personnelles est un concept large dans le cadre du RGPD Le RGPD régit la façon dont les données personnelles des individus de l'UE peuvent être traitées par les organisations. Les «données personnelles» et le «traitement» sont des termes fréquemment utilisés dans la législation, et la compréhension de leur signification particulière dans le cadre du RGPD éclaire la véritable portée de cette loi:

Les données personnelles sont des informations relatives à un individu identifié ou identifiable. Ce concept est très large car il inclut toute information pouvant être utilisée seule ou en combinaison avec d'autres informations pour identifier une personne. Les données personnelles ne sont pas seulement le nom ou l'adresse e-mail d'une personne. Il peut également englober des informations telles que des informations financières ou même, dans certains cas, une adresse IP. De plus, certaines catégories de données personnelles bénéficient d'un niveau de protection des données plus élevé en raison de leur nature sensible. Ces catégories de données concernent l'origine raciale et ethnique, les opinions politiques, les croyances religieuses et philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques, les données de santé, les informations sur la vie sexuelle ou l'orientation sexuelle et les antécédents criminels.

Traitement désigne toute opération ou ensemble d'opérations effectuées sur des données personnelles ou sur des ensembles de données personnelles, que ce soit par des moyens automatisés tels que collecte, enregistrement, organisation, structuration, stockage, adaptation ou altération, récupération, consultation, utilisation, divulgation par transmission, diffusion ou autrement mise à disposition, alignement ou combinaison, restriction, effacement ou destruction. Concrètement, cela signifie que tout processus qui stocke ou consulte des données personnelles est considéré comme un traitement. Concepts clés: contrôleurs de données et processeurs de données Dans la législation européenne sur la protection des données, deux types d'entités peuvent traiter des données personnelles: le contrôleur de données et le processeur de données.

Le responsable du traitement ("contrôleur") est l'entité qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel. Le processeur de données ("processeur") est l'entité qui traite les données personnelles pour le compte du contrôleur. Il est important de déterminer si l'entité traitant des données personnelles pour chaque activité de traitement de données est un contrôleur ou un processeur. Cet exercice de cartographie permet à une organisation de comprendre quels sont les droits et obligations attachés à chacune de ses opérations de traitement de données.

sceaduparadisier.fr a certaines activités de traitement de données pour lesquelles il agit en tant que contrôleur de données, et d'autres pour lesquelles il agit en tant que processeur de données.

Base légale pour le traitement des données personnelles dans le RGPD La considération suivante consiste à déterminer si une activité de traitement particulière est conforme à RGPD. Dans le cadre du RGPD, toute activité de traitement de données, exécutée en tant que contrôleur ou processeur, doit s'appuyer sur une base légale. Le RGPD reconnaît un total de six bases légales pour le traitement des

données personnelles des individus de l'UE (dans le RGPD, les personnes de l'UE sont appelées «personnes concernées»). Ces six bases juridiques, dans l'ordre de l'art. 6 (1) (a) à (f) RGPD, sont: La personne concernée a donné son CONSENTEMENT au traitement de ses données personnelles pour un ou plusieurs buts spécifiques;

Le traitement est NÉCESSAIRE POUR L'EXÉCUTION D'UN CONTRAT auquel la personne concernée est partie ou pour prendre des mesures à la demande de la personne concernée avant la conclusion d'un contrat;

Le traitement est nécessaire pour le RESPECT D'UNE OBLIGATION LÉGALE à laquelle le responsable du traitement est soumis;

LE TRAITEMENT EST NÉCESSAIRE POUR PROTÉGER UN INTÉRÊT VITAL DE LA PERSONNE CONCERNÉE.

LE TRAITEMENT DES DONNÉES EST NÉCESSAIRE À L'EXÉCUTION D'UNE TÂCHE EFFECTUÉE DANS L'INTÉRÊT PUBLIC OU DANS L'EXERCICE DE L'AUTORITÉ PUBLIQUE ;

ou le traitement est nécessaire pour les INTÉRÊTS LÉGITIMES poursuivis par l'entité, sauf si ces intérêts sont outrepassés par les intérêts ou les droits et libertés fondamentaux de la personne concernée qui requièrent la protection des données personnelles.

Il existe des similitudes entre la liste de traitement autorisée par le RGPD et la liste contenue dans la directive sur la protection des données. Cependant, il existe également des divergences significatives. La modification la plus fréquemment évoquée par le RGPD, par rapport à la directive sur la protection des données, est le durcissement des exigences de consentement (élément 1 de la liste ci-dessus). Les exigences de consentement du RGPD comprennent des éléments tels que (i) l'exigence que le consentement soit vérifiable, (ii) la demande de consentement doit être clairement distinguable des autres questions, et (iii) les personnes concernées doivent être informées de leur droit de retirer leur consentement. Il est également important de garder à l'esprit qu'une exigence de consentement encore plus élevée («consentement explicite») est imposée en ce qui concerne le traitement des données sensibles.

Un autre élément important à souligner est l'élément d'intérêt légitime (élément 6 de la liste ci-dessus). Lorsqu'elle s'appuie sur un «intérêt légitime» pour soutenir le traitement de données à caractère personnel, une organisation doit être consciente de l'exigence de test d'équilibrage associée à cette base juridique. Pour satisfaire au principe de responsabilité en vertu du RGPD, une organisation doit documenter sa conformité au test d'équilibrage, qui comprend son approche et les arguments qu'elle a examinés avant de conclure que le critère d'équilibrage était respecté.

Les droits des individus dans le cadre du RGPD En vertu de la directive sur la protection des données, les particuliers avaient la garantie de certains droits fondamentaux en ce qui concerne leurs données personnelles. Les droits des personnes continuent de s'appliquer dans le cadre du RPDG, sous réserve de

certaines modifications explicatives. Le tableau ci-dessous compare les droits des individus au titre de la directive sur la protection des données et du RGPD.

LE DROIT DE L'INDIVIDU DIRECTIVE SUR LA PROTECTION DES DONNÉES RGPD DEMANDE D'ACCÈS À UN SUJET DE DONNÉES Les individus ont le droit de savoir si leurs données personnelles sont traitées, ce qui et comment les données personnelles les concernant sont traitées et quelles sont les opérations de traitement des données. L'étendue de ce droit a été étendue dans le cadre du RGPD. Par exemple, lors d'une demande d'accès, les individus doivent recevoir des informations supplémentaires, y compris des informations sur leurs droits supplémentaires de protection des données dans le cadre du RGPD qui n'existaient pas auparavant, tels que le droit à la portabilité des données. DROIT D'OPPOSITION Un particulier peut interdire certaines opérations de traitement de données lorsqu'il a des motifs légitimes impérieux. Les particuliers peuvent également s'opposer au traitement de leurs données personnelles à des fins de marketing direct. Le RGPD a élargi la portée de ce droit par rapport à la directive sur la protection des données. DROIT DE RECTIFICATION OU D'EFFACEMENT Les personnes peuvent demander que des données incomplètes soient complétées ou que des données incorrectes soient corrigées pour garantir que le traitement des données personnelles soit conforme aux principes de protection des données applicables. La position du RGPD est matériellement la même que celle de la directive sur la protection des données, mais certaines protections procédurales sont renforcées dans le cadre du RGPD. DROIT À LA RESTRICTION Aucun droit de restreindre le traitement. Cependant, la directive sur la protection des données donne aux particuliers le droit de demander le blocage de leurs données personnelles lorsque les opérations de traitement ne respectent pas les principes de protection des données, par exemple lorsque les données sont incomplètes ou inexactes. Le RGPD offre aux particuliers le droit de demander la restriction du traitement de leurs données personnelles dans certaines circonstances, y compris lorsque l'individu conteste l'exactitude des données. DROIT D'EFFACEMENT ("DROIT D'ÊTRE OUBLIÉ") Les particuliers ont le droit de demander l'effacement de leurs données personnelles si les opérations de traitement n'étaient pas conformes aux principes de protection des données. Par conséquent, ce droit est très étroit. Le RGPD a considérablement élargi ce droit. Par exemple, le droit d'effacement peut être exercé lorsque des données personnelles ne sont plus nécessaires par rapport aux finalités pour lesquelles elles ont été collectées, ou que le particulier retire son consentement au traitement et qu'aucune autre base juridique ne justifie la poursuite du traitement. DROIT À LA PORTABILITÉ DES DONNÉES La directive sur la protection des données ne mentionne pas explicitement la «portabilité des données» comme un droit de la personne concernée. Les lois des États membres de l'UE ont peut-être mis en œuvre des droits supplémentaires s'apparentant à un droit de portabilité des données au niveau national. Les particuliers peuvent demander que des données personnelles détenues par un responsable du traitement soient fournies à eux-mêmes ou à un autre responsable du traitement. Transferts internationaux de données Le sujet des flux internationaux de données a été un sujet brûlant ces dernières années, et il y a eu un débat considérable et une réforme du droit dans ce domaine. Il est également certain que les lois entourant les flux internationaux de données continueront d'évoluer dans les années à venir. Aujourd'hui, selon la législation européenne sur la protection des données, certaines exigences doivent être satisfaites avant que les données personnelles des citoyens européens puissent être transférées en dehors de l'UE,

sauf si l'organisation recevant les données personnelles est située dans une zone de liste blanche.

Dans le cadre du RGPD, les transferts internationaux de données sont un sujet difficile à gérer car la loi évolue et il n'y a qu'un petit nombre de mécanismes de transfert de données disponibles. Malgré le défi, les organisations doivent rester au courant des développements car le flux conforme de données personnelles est l'épine dorsale de toute entreprise technologique. Un mécanisme particulièrement important pour les flux de données personnelles de l'UE vers les États-Unis est le cadre Privacy Shield. Le bouclier de confidentialité UE-États-Unis et Suisse-États-Unis est une méthode qui garantit qu'une organisation offre un niveau adéquat de protection des données, en exigeant qu'une organisation certifie et enregistre conformément aux exigences du cadre Privacy Shield.

De manière plus générale, sceaduparadisier.fr dispose de mesures internationales de conformité en matière de transfert de données qui régissent l'ensemble du traitement par Transipe des données personnelles des individus de l'UE. Ces mesures sont basées sur les clauses contractuelles standard de l'UE. Comme indiqué ci-dessus, les flux de données internationaux continuent d'être un domaine de réforme législative potentielle. Pour cette raison, nous suivons de très près les développements juridiques relatifs aux mesures internationales de conformité des transferts de données et nous prenons toutes les mesures à notre disposition pour assurer un transfert international conforme des données personnelles des personnes concernées. Cela signifie également que nous avons intégré les redondances dans notre programme de conformité du transfert de données dans toute la mesure du possible et que nous cherchons à les étendre avec les outils disponibles pour sceaduparadisier.fr dans le cadre du RGPD. Non-conformité La conséquence la plus mentionnée de la non-conformité avec le RGPD est l'amende maximale qui peut être imposée à une organisation non conforme. L'amende maximale pouvant être perçue est de 4% du chiffre d'affaires global ou de 20 millions EUR, selon le montant le plus élevé. Certains autres types d'infractions sont assortis d'une amende maximale de 2% du chiffre d'affaires global, soit 10 millions EUR, selon le montant le plus élevé.

Les pouvoirs des autorités de protection des données («DPA») en vertu de l'art. 58 du RGPD. Ces pouvoirs comprennent la possibilité pour les APD d'imposer des mesures correctives, telles qu'une limitation temporaire ou définitive des activités de traitement des données, y compris une interdiction complète du traitement des données, ou d'ordonner la suspension des flux de données à un destinataire dans un pays tiers.

Pour sceaduparadisier.fr et le RGPD la confidentialité, la protection des données et la sécurité des données sont au cœur de tout ce que nous faisons. Nous travaillons continuellement à rétablir la barre pour nous-mêmes dans le domaine de la sécurité et de la confidentialité des données, et considérons le RGPD comme une opportunité pour l'ensemble de l'industrie de se réunir et de s'améliorer.. La conformité RGPD comprend de nombreux éléments. Entre autres, nous mettons à jour notre documentation et nos accords pour les aligner sur les exigences du RGPD. Nous révisons également nos politiques et procédures internes afin de nous assurer qu'elles respectent la norme RGPD. La plupart des éléments de conformité du RGPD se déroulent «sous le capot» d'une organisation en ce qui concerne les mises à jour

sur la façon dont une organisation traite les données personnelles. Voici quelques-unes des étapes que les plates-formes comme sceaduparadisier.fr effectuent pour leurs utilisateurs (et eux-mêmes) en prévision du RGPD:

Effectuer une analyse des écarts entre les exigences imposées par la directive sur la protection des données et le RGPD, applicables aux activités commerciales de l'entreprise.

Examiner et mettre à jour les outils internes, les procédures et les politiques, au besoin.

Réviser les pratiques de mise en correspondance des données et d'inventaire des données et les mettre à jour au besoin pour se conformer aux obligations de conservation des documents en vertu du RGPD. Effectuer une analyse d'écart dédiée de l'outil de révision de la confidentialité et de la protection des données afin de répondre aux exigences de l'évaluation de l'impact de la protection des données. Mettre à jour l'approche des transferts internationaux de données.

Mettre à jour les contrats pour refléter l'Art. 28 obligations du RGPD en ce qui concerne les parties contractantes de la société.

Réviser et, le cas échéant, réviser les relations avec les fournisseurs afin de répondre aux exigences du RGPD pour s'assurer que ces tiers reçoivent et traitent les données personnelles de manière légale. Mettre à jour le programme de conformité de la vie privée de l'entreprise avec une formation continue des employés afin de refléter les changements à mettre en œuvre pour le RGPD.

Le principe de responsabilité Les utilisateurs de sceaduparadisier.fr devraient consulter leurs professionnels du droit pour comprendre l'étendue de leurs obligations de conformité dans le cadre du RGPD. En règle générale, si vous êtes une organisation établie dans l'UE ou si votre organisation traite des données personnelles de particuliers de l'UE, le RGPD s'appliquera à vous.

Un principe primordial de RGPD à garder à l'esprit est le principe de responsabilité. Le principe de responsabilité stipule que le responsable du traitement doit être en mesure de démontrer que ses activités de traitement sont conformes aux principes de protection des données énoncés dans le RGPD. La façon la plus simple de démontrer la conformité est de documenter et de communiquer votre approche de conformité RGPD.

Chez sceaduparadisier.fr la conformité a été le fruit d'une collaboration entre de nombreuses personnes au sein de notre organisation, notamment les opérations utilisateur, les ventes, l'ingénierie, la sécurité et le droit. D'après notre expérience, les partenariats inter-fonctionnels et la documentation facile à lire sont extrêmement utiles pour le processus global de conformité au RGPD.

Une liste de contrôle RGPD pour votre entreprise Il ne reste que quelques semaines avant le 25 mai 2018 pour que les petites et moyennes entreprises soient confrontées à des défis particuliers pour se préparer au RGPD. Dans cet esprit, nous

avons rassemblé certains des éléments clés d'un programme de conformité RGPD dans une liste de contrôle pour les utilisateurs.

✓vous sur la même page : Rassemblez-vous avec vos collègues techniques, de soutien à la clientèle et juridiques et mettez-vous au courant de ce qu'est le RGPD et de son impact sur votre organisation. ✓Obtenez une image claire de ce qui se passe avec les données personnelles dans votre organisation :

Un exercice de cartographie des données peut vous aider à découvrir comment les données personnelles sont stockées et traitées par vos systèmes. Les questions suivantes peuvent vous guider: Quelles sont les catégories de données personnelles que vous traitez? (p. ex. information financière, information sur la santé, information liée au marketing, etc.) Pour quelles catégories de personnes traitez-vous les données personnelles? (par exemple, titulaires de carte, enfants, patients, etc.) Quelle est la raison du traitement de cette information? Comment et pourquoi avez-vous recueilli cette information? Comment sécurisez-vous ces données? Des tiers reçoivent-ils cette information? Si oui, divulguez-vous ces destinataires tiers dans votre politique de confidentialité ou dans d'autres formes de notification? Savez-vous qui sont ces tiers? Combien de temps gardez-vous des informations sur les individus? ✓Cartographie des bases légales : Consulter les 6 bases légales mentionnées ci-dessus. Pour chaque opération de traitement identifiée dans votre carte de données, reliez-la à une base légale. Cette connexion vous donnera la carte de base légale.

✓Savoir respecter une personne exerçant ses droits:
Avoir la capacité d'utiliser les informations du mappage de données pour répondre à une demande d'accès de sujet de données. À partir de la carte de données, sachez où se trouvent les données personnelles dans votre système (et si vous faites des références croisées avec d'autres systèmes) pour vous conformer aux demandes d'exclusion, de modification et d'effacement. Sachez quels formats de données utilisent vos systèmes et déterminez comment vous allez répondre aux demandes de portabilité des données. ✓données et réponse aux incidents: Lorsque vous parlez à vos collègues du côté technique / sécurité de l'organisation, assurez-vous de connaître votre plan d'intervention en cas d'incident. Exécutez quelques exercices sur table pour que tous ceux qui participent à la réponse aux incidents sachent quoi faire en cas d'incident de sécurité. Idéalement, votre équipe de réponse aux incidents est une machine affinée, prête à exécuter des plans d'intervention en cas d'incident lorsque la situation se présente.

Il y a beaucoup d'autres éléments qui pourraient être ajoutés à cette liste de vérification, et vous devrez travailler avec vos experts internes et vos conseillers externes pour trouver une liste personnalisée selon vos besoins. Par exemple, vous devrez peut-être effectuer des évaluations d'impact sur la protection des données, nommer un responsable de la protection des données, gérer et réviser les pratiques de marketing et autres communications de l'entreprise, et revoir vos processus de gestion des fournisseurs.

Si vous avez une base solide en cartographiant vos activités de traitement de données, vous vous donnez un gros avantage pour toute question de conformité

RGPD ultérieure que vous rencontrez. Vous trouverez ci-dessous des ressources additionnelles que nous avons consultées et trouvées utiles, et nous espérons qu'elles vous seront également utiles.

Ressources additionnelles Le RGPD est mentionné dans de nombreux endroits différents, et il est difficile de garder une trace des bonnes ressources disponibles en ligne. Voici quelques ressources que nous consultons pour rester au courant des développements du RGPD: Tout commence par le texte légal : le texte légal complet du RGPD est ici et la directive sur la protection des données est liée ici .

L'Autorité de surveillance : Il existe une Autorité de protection des données (DPA) dans chaque Etat membre de l'UE, et beaucoup d'entre eux ont publié des lignes directrices utiles sur la mise en œuvre du RGPD. Vous trouverez une liste des DPA ici .

Groupe de travail «Article 29» (WP29), qui deviendra bientôt le comité européen de la protection des données (EDPB) : Le WP29 est un organe consultatif composé d'un représentant du DPA de chaque État membre de l'UE, du contrôleur européen de la protection des données et de la Commission européenne. À compter du 25 mai 2018, le WP29 deviendra l'EDPB. L'EDPB comprendra le chef d'un DPA de chaque État membre de l'UE et le contrôleur européen de la protection des données. Le WP29 a publié des centaines de lignes directrices et d'avis et a ouvert plusieurs sujets de consultation. Les lignes directrices et les opinions les plus récentes se concentrent sur la meilleure façon de mettre en œuvre les éléments du RGPD dans la structure de conformité d'une organisation. La salle de presse WP29 est ici .

L'ancien site web du groupe de travail 29 avait beaucoup de ressources supplémentaires qui ne sont malheureusement plus aussi facilement accessibles avec la nouvelle mise en page du site. Le site web archivé avec des matériaux supplémentaires est disponible ici . Certains DPA, cabinets d'avocats, organismes de protection de la vie privée tels que l' IAPP , et de nombreuses autres organisations, ONG et entreprises organisent des événements liés au RGPD. Il est très probable que d'autres organisations ont des questions très similaires à la vôtre concernant la mise en œuvre du RGPD. Ce sont de formidables opportunités d'atteindre la communauté RGPD et de travailler ensemble sur les questions.