Les fondamentaux du GDPR et comment PwC peut vous aider

Résumé – Règlement général sur la protection des données

Adoption par l'UE de règles de protection des données plus strictes

Le Règlement général sur la protection des données (GDPR) est entré en vigueur le 24 mai 2016. Il crée un nouveau cadre réglementaire unifiant les lois de protection des données dans les 28 pays membres de l'Union européenne (UE) et remplace la précédente Directive sur la protection des données personnelles de l'UE. Le GDPR impose une protection des données radicale et un cadre réglementaire de protection de la vie privée en Europe et dans le monde entier pour le traitement des données à caractère personnel des citoyens de l'UE. Bien que les pays et les entreprises aient deux ans pour se préparer, les entreprises devraient commencer à agir sans tarder pour pouvoir répondre aux nombreuses exigences nouvelles et nettement renforcées, avant la date butoir de mai 2018.

Les sociétés suisses sont-elles concernées ?

Le GDPR a une portée beaucoup plus large que la précédente directive de l'UE sur la protection des données et signifie que la nouvelle loi s'applique directement à davantage d'entreprises. Toutes les entreprises qui sont actives en Europe devront se conformer au GDPR. Cela inclut les entreprises qui n'ont pas d'établissement dans l'UE mais qui procurent des marchandises et des services aux personnes résidentes de l'UE ou qui y surveillent des gens. Par exemple, un revendeur suisse qui n'a pas d'établissement dans l'UE mais envoie des produits à des clients basés dans l'UE devra se conformer au GDPR.

Un parcours vers la conformité

Le GDPR contient une série de nouvelles règles qui exigent que les entités revoient et renouvellent leurs systèmes et leurs opérations de protection des données. Collectivement, ces nouvelles règles définissent un nouveau « parcours vers la conformité » que les entités devront suivre pour rester du bon côté de la loi.

Sans aucun doute, le GDPR représente une grande problématique pour de nombreuses entités et en particulier celles qui collectent de grandes quantités de données à caractère personnel ou ont des business models basés sur l'exploitation commerciale des données à caractère personnel.

pwc

Le parcours vers la conformité implique d'innombrables défis et la tâche est complexe. Les entités peuvent trouver qu'elles ont des choix difficiles à faire pour faire avancer leurs priorités. Garantir la conformité avec le GDPR demandera des ressources considérables et beaucoup de planification.

Les risques réglementaires et de litiges sévères sont considérables et en particulier pour les entités qui traitent des données à caractère personnel sensibles.

Ces règles arrivent à un moment où la tension est très forte dans l'environnement des transferts de données internationaux, suite à des litiges récents et très médiatisés. Les entités auront besoin d'assurer que les modèles de partage et de transfert de données globaux sont adaptés sur le plan opérationnel en cas de contestation.

Le GPDR est un changement important, il intègre des obligations qui doivent être prises en compte avec soin.

Pourquoi les responsables de la sécurité des systèmes d'information (RSSI) doivent-ils se sentir concernés?

L'adoption du GDPR représente pour les RSSI de nombreuses entreprises partout dans le monde de nouveaux et nombreux défis. Voici un aperçu des principales problématiques :

- Définition plus large des « données à caractère personnel »

  Selon le GDPR, les données à caractère personnel sont toutes les informations en lien avec une personne physique identifiée ou identifiable (« personnes concernées »).

  Cette définition des données à caractère personnel est importante pour les professionnels de la sécurité de l'information parce qu'elle implique des données qui ne semblent pas, à première vue, pouvoir être considérées comme personnelles. Les adresses IP, les identifiants d'application, les données des systèmes de navigation (GPS), les cookies, les adresses physiques des cartes réseau (adresses MAC), les identifiants uniques d'appareils mobiles (UDID), et le numéro de série des équipements mobiles (IMEI) en sont des exemples.

- Etablissement de normes de protection des données

  Le GDPR exige que les sociétés mettent en œuvre les mesures techniques et organisationnelles nécessaires pour garantir un niveau de sécurité approprié aux données à caractère personnel qu'elles détiennent. Le règlement stipule expressément que ces mesures incluent :

  – la pseudonymisation et le chiffrement des données à caractère personnel ;
  – des moyens permettant de garantir en tout temps la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement ;
  – des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; et
  – une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

- De nouvelles exigences de notification en cas de violation des données

  Le GDPR introduit un mécanisme de mise à l'index par lequel les entreprises devront notifier aux autorités compétentes en matière de protection des données s'il y a un incident de sécurité qui affecte la sécurité des données à caractère personnel qu'elles détiennent.

  La notification doit être faite dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Si la notification n'est pas faite dans les 72 heures, les entreprises doivent donner le motif justifié de ce retard.

  Si la violation peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, ou à tout autre dommage économique ou social important pour les personnes concernées, les entreprises devront notifier la violation aux personnes concernées. Il est important de noter qu'aucune notification aux personnes concernées ne sera requise si les entreprises ont mis en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour les données qui ont été affectées par la violation. Ainsi, si, avant la violation, les données ont été rendues incompréhensibles, par exemple par un chiffrement, les entreprises ne sont pas tenues de notifier cette violation aux personnes concernées.

- Le coût élevé des défaillances

  L'UE veut que les nouvelles règles de protection des données deviennent une question abordée au plus haut niveau de l'entreprise et elle a donc décidé de rendre les infractions passibles de lourdes amendes :

  – si une entreprise ne se conforme pas aux obligations en matière de sécurité des données stipulées dans le GDPR, elle peut recevoir une amende pouvant aller jusqu'à 10'000'000 € ou jusqu'à 2% de son chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu.

  – Pire encore, si une entreprise est repérée en violation de certaines autres obligations relevant du GDPR, l'amende peut s'élever à un montant impressionnant de 4% de son chiffre d'affaires annuel mondial total.

Comment PwC peut vous aider ?

En tant qu'organisation multidisciplinaire, nous sommes particulièrement bien placés pour aider nos clients à s'adapter à un nouvel environnement. Notre équipe de protection des données comprend des avocats, consultants, spécialistes de la cybersécurité, auditeurs, spécialistes des risques, experts en investigation numérique légale et stratèges. Notre équipe est vraiment globale, elle propose des solutions innovantes et possède une expertise sur le terrain dans toutes les plus grandes économies de l'UE. Notre gamme de services inclut entre autres :

- Évaluation de la maturité

  Nous avons développé un sondage interactif présentant le niveau de risques pour évaluer la maturité GDPR de nos clients en optimisant les coûts.

  Le sondage s'établit autour d'environ 60 questions-clés, avec des réponses préremplies en lien avec notre matrice de maturité. Les personnes interrogées sélectionnent des niveaux de maturité selon différents critères en relation avec le cadre de conformité établi au sein de leur entreprise, et du respect des principes de protection des données édictés dans le GDPR.

  L'outil génère un rapport contenant une évaluation des risques en fonction des différents niveaux de maturité indiqués par les personnes interrogées. Les risques sont évalués en référence aux tendances en termes de risques et de mise en œuvre réglementaires, en termes de satisfaction des consommateurs et des employés, de risques de litige et des risques B2B en relation avec des tiers et des entités externalisées.

- Inventaire des données à caractère personnel

  Les régulateurs mondiaux et le grand public sont de plus en plus sensibles aux questions de protection des données personnelles. Dans cette optique, le GDPR demande aux entreprises de faire des efforts pour prouver leur conformité opérationnelle et leur responsabilité. Une telle exigence demande une solide compréhension des opérations sur les données globales. Ceci n'est possible que par un effort de communication et d'inventaire des données et l'application de bonnes pratiques pour tenir à jour l'inventaire des données au fil du temps.

Nous avons développé des modèles personnalisables et adaptables et des outils pour faciliter la collecte directe d'informations pour l'inventaire des données-clés et pour définir les efforts de traitement des données dans une entreprise.

- Gap analysis complet

  Nous avons aussi établi une méthode plus complète spécifiquement conçue pour évaluer le degré de maturité des capacités de protection des données d'une entreprise et identifier les écarts par rapport aux exigences du GDPR. Notre méthode éprouvée d'analyse des écarts, inclut 41 contrôles regroupés dans les huit domaines suivants:

1. Stratégie, gouvernance et responsabilité
2. Droits des personnes concernées et traitement
3. Déclaration de confidentialité et gestion des politiques
4. Gestion des risques et conformité
5. Gestion du cycle de vie des données
6. Réponse aux incidents et gestion des violations
7. Gestion des risques pour les tiers
8. Protection des données

- À la fin de l'évaluation, nous fournissons un rapport qui contient les éléments suivants :
  - un résumé de vos capacités-clés, soulignant vos forces en matière de protection des données ;
  - un résumé de vos principales faiblesses, décrivant les domaines d'amélioration pour être conforme au GDPR (p. ex. les caractéristiques de confidentialité les plus en pointe dans le secteur par rapport à votre statut) ;
  - votre maturité actuelle, par rapport aux exigences du GDPR en matière de risques et aux meilleures pratiques du secteur ;
  - nos recommandations pour améliorer vos capacités de protection des données et être conforme au GDPR ; et
  - notre évaluation sur le niveau d'effort nécessaire pour répondre aux exigences du GDPR.

- Développement d'un plan d'action

  Nous avons une grande expérience dans la conception de programmes de confidentialité. Nous pouvons vous aider à concevoir vos capacités futures de protection des données en développant un ensemble de recommandations pragmatiques, ainsi que les plans d'action associés et la feuille de route de la mise en œuvre, pour combler les écarts constatés par rapport aux exigences du GDPR. Ainsi, vous verrez clairement votre statut actuel, les objectifs à atteindre et comment vous pouvez combler les écarts existants.

- Assistance dans l'implémentation des actions de mise en conformité

  Nous avons développé une solide expertise dans le conseil pour nos clients sur les stratégies de conformité, les audits et l'assurance. Nous pouvons vous aider à mettre en œuvre une large variété d'actions pour arriver à la conformité avec le GDPR, en mobilisant notre réseau mondial d'avocats, de consultants informatiques et de spécialistes des audits et des risques. De plus, l'un des principaux défis auquel sont confrontées les sociétés qui suivent des programmes de transformation en matière de protection des données est de gérer la complexité, les interdépendances et le séquencement des activités. Nous avons une longue expérience dans la gestion de programmes complexes et avons développé des outils et des modèles spécialement conçus pour aider à surmonter les défis associés.

Notre réseau mondial d'experts en cybersécurité et protection des données personnelles

Contacts

Reto Häni
Cybersecurity Partner and Leader
PwC Digital Services
+41 79 345 01 24
reto.haeni@ch.pwc.com

Andrea Gergen
Cybersecurity as a Service, Data Protection and Regulatory Compliance
PwC Digital Services
+41 79 419 25 07
andrea.gergen@ch.pwc.com

Susanne Hofmann-Hafner
Legal Compliance Leader
PwC Tax and Legal Services
+41 58 792 17 12
susanne.hofmann@ch.pwc.com