UE-GDPR : êtes-vous prêts ?

Notre solution pour répondre à vos interrogations sur le GDPR

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

- Le Parlement européen a approuvé le 14 avril 2016 le Règlement général sur la protection des données (GDPR). Celui-ci crée un nouveau cadre réglementaire unifiant les lois sur la protection des données dans les 28 pays membres de l'Union européenne (UE) et remplace la directive européenne actuelle relative à la protection des données.
- Le GDPR n'entrera pas en vigueur avant mai 2018. Cependant, de nombreuses exigences nouvelles ou modifiées de manière significative requièrent d'agir avant cette date.
- En tant qu'organisation multidisciplinaire, nous sommes particulièrement bien placés pour aider nos clients à s'adapter à ce nouvel environnement. Notre équipe spécialisée dans la protection des données comprend des avocats, des consultants, des auditeurs, des spécialistes des risques, des experts en criminalistique et des stratèges. Notre équipe est véritablement internationale et offre une expertise de terrain dans toutes les grandes économies de l'UE.

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, ce qui signifie que la nouvelle loi s'applique directement à davantage d'entreprises. Toutes les entreprises avec des activités en Europe devront se conformer au GDPR. Cela inclut les entreprises qui n'ont pas d'établissement dans l'UE mais qui fournissent 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.

Êtes-vous prêts ? Effectuez l'évaluation de votre maturité GDPR

- Planifiez une demi-journée avec l'un de nos spécialistes de la protection des données personnelles pour effectuer une évaluation de votre maturité GDPR en utilisant notre sondage interactif.
- Le sondage comporte environ 60 questions-clés sur la protection des données, avec des réponses pré-remplies en lien avec notre matrice de maturité. Les personnes interrogées sélectionnent des niveaux de maturité selon différents critères en relation avec le cadre de

pwc

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 réglementaire, de satisfaction des consommateurs et des collaborateurs, de risques de litige et de risques B2B en relation avec des tiers et des entités externalisées.

Notre approche

1. Exigences GDPR

Par différents aspects, le GDPR est plus atreignant que la précédente réglementation sur la protection des données personnelles, la directive sur la protection des données. Il comprend de nouvelles exigences d'importance en matière de gouvernance des données et sur la manière dont celles-ci sont utilisées, collectées, conservées et partagées. Il comporte également un alourdissement conséquent des pénalités en cas de non-respect.

Pour vous assurer d'être bien informés sur les dernières exigences de l'UE, nous commencerons par une brève introduction qui soulignera les points-clés de la nouvelle réglementation, sur la base d'une analyse approfondie menée par notre réseau mondial d'experts.

2. Évaluation

L'évaluation comporte une série de questions. Quatre réponses, correspondant chacune à un degré de maturité, sont proposées pour chaque question. Les degrés de maturité vont de 1 (maturité faible indiquant un niveau de conformité bas) à 4 (indiquant un positionnement complet et pleinement optimisé en matière de conformité). Les questions du sondage sont formulées de manière à évaluer les éléments de deux domaines-clés :

- Architecture de protection des données – évaluation des structures en place au sein de l'organisation pour favoriser la conformité.

Pour vous aider à comprendre les niveaux de maturité, les deux domaines cités ci-dessus sont divisés en une série de sous-domaines. Le niveau de maturité est indiqué pour toutes les questions dans chaque sous-domaine.

Les sous-domaines sont listés ci-dessous.

Architecture de protection des données	• Périmètre territorial • Vision et stratégie • Conception de programme • Gouvernance	• Rôles et responsabilités dans la protection des données • Registres • Politiques	• Conception • Contrôles • Formation et sensibilisation • Garantie	• Tiers • Remise en cause • Responsabilité • Remédiation
Principes de protection des données	• Légalité, impartialité et transparence	• Limitation de la finalité • Minimisation des données	• Exactitude • Limitation du stockage	• Intégrité et confidentialité • Droits • Transferts

- Principes de protection des données – évaluation de la maturité opérationnelle pour l'application des principes de protection du GDPR.

  La valeur du rapport dépend de la qualité des informations que vous nous fournissez. La sélection appropriée des personnes appelées à participer à cette évaluation est essentielle à l'obtention d'un rapport de qualité. C'est pourquoi nous demandons aux personnes interrogées de tirer parti de leur connaissance et leur expérience de l'organisation pour déterminer la maturité du positionnement de l'entité en matière de conformité sur la matrice de maturité en réponse à chaque question. Les personnes sélectionnées pour participer à cette évaluation devraient idéalement travailler dans les domaines suivants :
- Juridique/Conformité – collaborateur connaissant l'architecture de conformité en place dans votre organisation.
- Gestion de l'information – collaborateur connaissant la gestion du cycle de vie de l'information, de la collecte à la suppression définitive.
- Sécurité de l'information – collaborateur connaissant les mesures techniques et organisationnelles en place pour sécuriser les données, notamment la détection des violations et la réaction à celles-ci.

Notre outil d'évaluation de la maturité GDPR ne garantit pas l'exactitude des informations que vous nous fournissez.

3. Analyse

Chaque sous-domaine correspond à un thème lié à une série de questions conçues pour évaluer les aspects adéquats sur ce sujet. L'outil d'évaluation de la maturité GDPR relie chaque question aux articles et considérants du GDPR. Ceci nous permet de synthétiser votre niveau de maturité – votre degré de préparation – par rapport au GDPR.

Par ailleurs, notre équipe d'évaluation recueillera des informations complémentaires en lien avec chaque question durant le processus d'évaluation. Ces informations serviront à ajouter des éléments de contexte à la synthèse des résultats pour votre organisation.

4. Reporting

Notre rapport vous fournira une synthèse de haut niveau sur le positionnement de votre organisation en matière de conformité dans les deux domaines de l'« architecture de protection des données » et des « principes de protection des données ». Une vision plus détaillée vous montrera ensuite la maturité de tous les sous-domaines évalués.

Le rapport reprendra toutes les questions posées et le positionnement de l'organisation sur la matrice de sécurité suivant les réponses des participants au sondage. Le rapport indique également à quels articles et considérants du GDPR se rapporte chaque question.

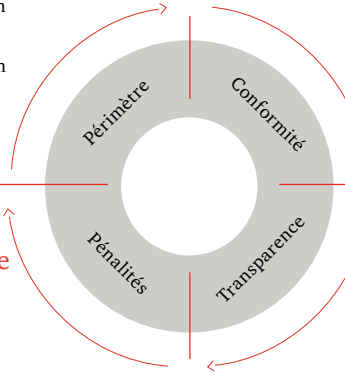
Pour plus d'informations sur les bénéfices que vous pouvez tirer de cette nouvelle offre particulièrement intéressante, veuillez vous adresser aux personnes indiquées dans la rubrique Contacts.

Extension du périmètre

- Entités concernées plus nombreuses
- Entités de traitement des données soumises à une réglementation renforcée
- Entités de traitement ou de contrôle non UE soumises à la réglementation
- Directement applicable pour tous les pays membres de l'Union européenne, sans qu'un pays ait besoin d'un texte de transposition spécifique
- Nouveaux principes de protection des données

Obligations renforcées en matière de conformité

- Prise en compte du respect de la vie privée dès la conception (« privacy by design »)
- Études d'impact sur la vie privée
- Obligations relatives à la responsabilité, notamment plans de conformité, audits réglementaires et inspections
- Contrôles de l'utilisation, par exemple « droit à l'oubli », portabilité des données, minimisation des données
- Responsables de la protection des données
- Nouvelles exigences en matière de profilage des clients, telles que la nature du consentement



Risques de sanctions et de litiges

- Pouvoirs de contrainte étendus
- Amendes pouvant aller jusqu'à 4 % du chiffre d'affaires mondial annuel ou 20 millions d'euros
- Demandes d'indemnisation et demandes d'indemnisation multi-tiers

Plus grande transparence

- Consentement explicite
- Protection des enfants
- Politiques de respect de la vie privée
- Consultation des parties prenantes
- Divulgation des violations
- Nouvelles règles pour l'utilisation des données, par exemple interdiction des propositions commerciales liées et de l'agrégation de données

Contacts

Reto Haeni
Cyber Security Partner and Leader, PwC Digital Services
+41 79 345 01 24
reto.haeni@ch.pwc.com

Nicolas Vernaz
Data Protection and Regulatory Compliance Lead, PwC Digital Services
+41 79 419 43 30
nicolas.vernaz@ch.pwc.com

Susanne Hofmann-Hafner
Legal Compliance Lead, PwC Tax and Legal Services
+41 79 286 83 67
susanne.hofmann@ch.pwc.com