Développements réglementaires

Autres évolutions récentes en matière de réglementation

Dernière mise à jour : mai 2024

pwc

Table des matières

1 Autres développements

1.1 Règlement général sur la protection des données de l'UE (RGPD)

Le RGPD de l'UE met en œuvre un cadre juridique strict pour la protection des données et de la vie privée en Europe et en dehors de l'Europe en ce qui concerne le traitement des données personnelles. Le règlement a été repris par les États de l'EEE.

Statut :
- En vigueur depuis le 25 mai 2018

Applicabilité de dispositions européennes plus strictes en matière de protection des données

Le Règlement général sur la protection des données (RGPD) de l'UE est en vigueur depuis le 25 mai 2018. Il a créé un nouveau cadre juridique pour les lois sur la protection des données dans les 28 États membres de l'Union européenne (UE) et a remplacé la précédente directive européenne sur la protection des données.

Le RGPD de l'UE met en œuvre un cadre juridique strict pour la protection des données et de la vie privée en Europe et en dehors de l'Europe en ce qui concerne le traitement des données personnelles. Par décision du Comité mixte de l'EEE du 6 juillet 2018, le RGPD a été intégré à l'accord EEE et est également applicable en Islande, en Norvège et dans la Principauté de Liechtenstein depuis le 20 juillet 2018.

Parcours de conformité

Les nouvelles dispositions du RGPD de l'UE exigent que les entreprises fassent le point sur leurs systèmes et processus opérationnels et les adaptent en matière de protection des données. Dans leur ensemble, les règlements établissent un « parcours de compliance » que les organisations doivent suivre pour garantir le respect des prescriptions. Le RGPD de l'UE représente un défi majeur et complexe pour de nombreuses entreprises, en particulier celles qui disposent d'archives volumineuses, de nombreuses entreprises tierces/de sous-traitants chargés du traitement des données et de systèmes informatiques complexes. La mise en œuvre des exigences comporte de nombreux défis et est souvent très complexe. Les risques réglementaires et opérationnels sont importants, en particulier pour les entreprises dont l'activité repose sur l'utilisation commerciale de données à caractère personnel.

Des infractions graves ont déjà été sanctionnées par des amendes de plus de EUR 200 millions. Des montants de plusieurs millions ne sont pas rares pour les grandes entreprises. Les violations du règlement peuvent être sanctionnées par une amende pouvant aller jusqu'à EUR 20 millions ou 4% du chiffre d'affaires annuel (éventuellement au niveau mondial) – le montant le plus élevé étant retenu. Le RGPD de l'UE réglemente également le transfert international de données. Les transferts de données transfrontaliers sont soumis à des conditions strictes qui doivent être analysées. Les organisations ont la responsabilité de sécuriser de manière adéquate les transferts de données transfrontaliers. Cela s'applique à la fois aux transferts existants et aux nouveaux transferts de données à caractère personnel, en particulier vers les pays dits « tiers » (pays hors UE et EEE).

Les principes de protection des données du RGPD de l'UE doivent toujours être respectés. Des principes tels que la limitation de la conservation, la minimisation des données ou la licéité font partie de la norme de protection des données dans le cadre du traitement des données personnelles. Il existe également un « principe de responsabilité », qui exige que les entreprises soient en mesure de démontrer qu'elles respectent le RGPD de l'UE. Cela s'applique d'une part aux autorités de protection des données, mais est aussi de la plus haute importance pour les parties prenantes internes ou externes. Les droits des personnes

concernées (« data subjects ») doivent également être pris en compte en temps utile. En particulier le droit à l'oubli ainsi que le paysage informatique parfois très complexe au sein d'une organisation posent des défis considérables aux entreprises.

Le RGPD de l'UE constitue une innovation importante dans la législation sur la protection des données. Même après la fin de la période de transition de deux ans et la mise en œuvre dans l'entreprise, les développements ultérieurs devront encore être soigneusement analysés. Les activités des autorités de contrôle et la législation sur la protection des données exigent une surveillance continue et institutionnalisée de la part de l'entreprise.

Qui est concerné ?

Le champ d'application du RGPD de l'UE va plus loin que la précédente directive européenne sur la protection des données. Toute organisation active en Europe qui traite des données à caractère personnel doit se conformer aux dispositions du RGPD de l'UE. Cette règle s'applique également à celles qui, bien que non établies dans l'UE, offrent des biens et des services à des personnes dans l'UE ou surveillent des personnes qui se trouvent dans ses États membres. Ainsi, par exemple, un commerçant suisse ne possédant pas de succursale dans l'UE mais dont les activités de marketing visent des acheteurs dans l'UE doit se conformer aux dispositions du RGPD de l'UE. Il en va de même pour les entreprises qui offrent leurs produits et services dans l'EEE ou qui surveillent des personnes dans ses États membres.

Ce que vous devez faire

Maintenant que le RGPD est entré en vigueur, on peut supposer que vous avez déjà mis en œuvre une grande partie des nouvelles exigences dans votre entreprise.

Nous recommandons donc les étapes suivantes :

- Identification des écarts entre votre programme actuel de protection des données et les exigences du RGPD, en tenant compte également de vos sous-traitants chargés du traitement des données ;
- Adaptation et amélioration des structures opérationnelles pour assurer le respect des prescriptions ; cela inclut une documentation complète de vos processus de protection des données ainsi que des contrôles appropriés ;
- Des contrôles et certifications en matière de protection des données doivent être envisagés pour démontrer le respect des règles de compliance en interne et en externe.

Votre expert PwC en protection des données se fera un plaisir de vous aider à élever votre niveau de protection et à assurer le respect du principe de responsabilité.

1.2 Révision de la loi fédérale sur la protection des données (nLPD)

La législation suisse sur la protection des données est en cours de révision, notamment la nLPD et l'ordonnance relative à la LPD (OLPD). La nLPD prend pour modèle le Règlement général sur la protection des données de l'UE, avec toutefois quelques différences importantes.

Statut :
- Entrée en vigueur le 1er septembre 2023

Révision de la loi sur la protection des données

Le 15 septembre 2017, le Conseil fédéral a publié le projet de révision de la loi fédérale sur la protection des données (P-LPD). Cette révision de la loi vise à renforcer la protection des données à caractère personnel et à adapter les dispositions existantes à l'ère numérique. Elle a également pour but d'adapter la loi suisse sur la protection des données à la législation européenne, c'est-à-dire au Règlement général sur la protection des données de l'UE (RGPD UE). Presque trois ans après la publication de la première mouture, le projet de

loi a désormais été adopté le 25 septembre 2020 par le Conseil national et le Conseil des États, après plusieurs divergences et une commission de conciliation entre les deux conseils nationaux.

Un facteur qui a caractérisé la révision de la LPD pendant les trois années de délibérations a été la garantie d'un accès illimité au marché intérieur européen. Suite à la pression exercée par la Commission européenne dans cette affaire, certaines parties de la législation européenne sur la protection des données semblent maintenant avoir été volontairement transposées en droit suisse. L'objectif était de garantir que la Suisse continue à être considérée par l'UE comme un pays tiers offrant une protection adéquate des données et puisse ainsi bénéficier de transferts de données transfrontaliers sans mesures de protection juridique supplémentaires.

Éléments clés du projet de loi et différences par rapport au RGPD de l'UE

À l'instar du RGPD de l'UE, le projet de loi suisse vise avant tout à améliorer la transparence du traitement des données et à renforcer les sanctions pénales en cas de violation de la protection des données. Le projet reprend d'ailleurs la terminologie juridique de l'UE dans divers domaines.

Par ailleurs, il poursuit une approche basée sur le risque. Ainsi, par exemple, les obligations du responsable des données en matière de protection des données augmentent en fonction des risques pour la sphère privée des personnes concernées. Tout comme le RGPD de l'UE, la loi révisée prévoit essentiellement que tous les responsables des données et les personnes assurant leur traitement sont tenus de documenter leurs activités en lien avec le traitement des données (registre des activités de traitement). En outre, conformément à l'évolution au sein de l'UE, le P-LPD renforce le rôle et la position du Préposé fédéral à la protection des données et à la transparence (PFPDT).

Dans certains domaines, le projet de loi diffère toutefois fondamentalement du droit européen. Ainsi, par exemple, il ne prévoit pas l'obligation pour les responsables des données de documenter le respect du P-LPD selon le principe de responsabilité. Contrairement au RGPD de l'UE, il n'y a donc pas de renversement de la charge de la preuve en matière de protection des données. De même, le projet de loi ne comporte aucune disposition spécifique sur la protection des enfants.

D'autres différences par rapport au RGPD de l'UE résident dans les sanctions pénales. Le montant maximum des amendes est de CHF 250'000, ce qui est nettement inférieur aux montants prévus au sein de l'UE. Par ailleurs, conformément au P-LPD, les poursuites pénales continuent de s'appliquer aux collaborateurs responsables (personnes physiques), alors que dans l'UE, elles s'appliquent aux services responsables (entreprises).

Conséquences de la révision et entrée en vigueur

Comme l'adoption de la nouvelle loi sur la protection des données représente une étape majeure dans l'adaptation des mesures de protection des données de la Suisse souhaitée par la Commission européenne, le risque que l'UE les juge insuffisantes est désormais relativement faible. La Suisse devrait donc continuer à être reconnue par l'UE comme équivalente dans le domaine de la protection des données. Ceci est particulièrement important pour l'économie suisse.

Ce que vous devez faire

Nous recommandons vivement aux entreprises de se pencher dès à présent sur les nouvelles dispositions de la loi sur la protection des données personnelles, notamment si elles n'ont pas pris de mesures concernant le RGPD de l'UE.

Les entreprises opérant en Suisse doivent acquérir une compréhension complète de la façon dont elles traitent les données à caractère personnel. Suite à cette analyse et en adoptant une approche basée sur les risques, les mesures nécessaires devraient être prises pour garantir que le traitement des données personnelles est conforme à la future loi. Votre expert PwC en protection des données peut vous aider à vous adapter au nouvel environnement.

2 International Standards on Auditing (ISA)

2.1 ISA 600 (révisée) « Audits d'états financiers de groupe (y compris l'utilisation des travaux des auditeurs des composants) – Considérations particulières »

La norme renforce et étend les responsabilités du responsable de la mission du groupe pour la gestion et l'atteinte de la qualité de l'audit sur la mission, ainsi que les responsabilités de l'auditeur du groupe pour la direction et la supervision générales de l'audit du groupe et la revue des travaux des auditeurs des composants.

Statut :	• Applicable aux audits d'états financiers pour les périodes commençant le ou après le 15 décembre 2023

Les modifications les plus importantes apportées à la norme sont les suivantes :

- La responsabilité de l'auditeur du groupe pour l'audit du groupe ainsi qu'un changement dans la définition de l'équipe de mission.
- L'auditeur du groupe doit déterminer les composants dans lesquels les travaux d'audit seront effectués (à cette fin, la notion de « composants importantes » et l'« examen limité de l'information financière du composant » comme type de travail ont été supprimés) ainsi que la nature, le calendrier et l'étendue de l'implication des auditeurs des composants.