La loi suisse sur la protection des données a été révisée et adoptée par le parlement suisse à l'automne 2020. Elle se fonde sur le Règlement général de l'UE sur la protection des données (RGPD-UE) mais s'en écarte sur quelques points. Les modifications devraient entrer en vigueur dans le courant de l'année 2022.

La révision de la loi sur la protection des données (nLPD) doit garantir une plus grande transparence concernant l'utilisation des données personnelles et renforcer le droit de codécision des personnes dont les données sont traitées. La loi prévoit entre autres la suppression des données personnelles lors de l'abandon de l'activité de traitement, notamment en cas de clôture d'une relation d'affaires.

Les nouveautés sont décrites en détail ici, par exemple (article de Netzwoche), c'est pourquoi nous ne mentionnons que brièvement les principales modifications:

- Renforcement des droits des personnes concernées, notamment grâce à une plus grande transparence (information sur le traitement des données)
- Encouragement de la prévention et de la responsabilité propre des personnes chargées du traitement des données
- Renforcement de la surveillance de la protection des données (par le Préposé fédéral à la protection des données et à la transparence PFPDT)
- Développement des dispositions pénales

Les conséquences pour les entreprises s'occupant du traitement des données en Suisse ne doivent pas être sous-estimées. La nLPD concerne aussi bien les banques en tant que responsables de leurs données clients (personnelles) que les entreprises d'externalisation en tant qu'exploitantes d'applications contenant des données personnelles. Les entreprises devront catégoriser et classifier (plus) précisément les données personnelles et procéder à une inventorisation des systèmes afin que des mesures en ce sens puissent être mises en œuvre pour le traitement des données.

La mise en œuvre de la nLPD nécessite donc un travail d'analyse et de conception détaillé avant de pouvoir procéder à des adaptations techniques dans les applications concernées ainsi qu'à d'éventuelles modifications structurelles. Plus encore, la nLPD concerne l'ensemble de l'entreprise : le front- et back-office, Compliance et Legal, les éventuels partenaires d'externalisation, et jusqu'à la direction et au conseil d'administration en tant qu'organes responsables.

Comment aborder concrètement la mise en œuvre des nouvelles exigences ?

Registre des activités de traitement

L'élément central lors de la première étape est l'établissement du registre des activités de traitement qui recense les différentes finalités des traitements et les applications correspondantes. Il s'agit d'avoir pour commencer une compréhension commune de ce que sont les données personnelles - les données personnelles ne doivent pas toutes être traitées avec le même soin dans le cadre de la nLPD.

Le registre des activités de traitement contient notamment les indications suivantes:

- responsable/personne chargée du traitement;
- finalité(s) du traitement;
- motifs justifiant le traitement;
- devoir d'information du client;
- provenance des données;
- catégories de personnes concernées et catégories de données personnelles traitées;

Août 2021 | Silvan Lohri, Head Consulting Swisscom Banking | Swisscom Business Customers

- traitement de données personnelles particulièrement sensibles;
- délai de conservation;
- mesures visant à garantir la sécurité des données;
- applications dans lesquelles est effectué le traitement.

Par expérience, le registre des activités de traitement doit être détaillé de manière suffisamment pragmatique : les traitements peuvent être saisis par exemple suivant les processus bancaires principaux Signalétique client, le trafic des paiements, placements, financement et prévoyance avec des compléments spécifiques (par exemple traitements dans le cadre d'activités de marketing).

Une liste des applications avec les données qui y sont traitées (classées en CID, CID de masse et non critiques) et des informations sur la conservation persistante des données aident ensuite à définir la priorité de l'application à traiter.

Les projets que nous avons réalisés avec les banques montrent qu'une approche pragmatique est judicieuse: les données personnelles ne peuvent pas toutes être supprimées dès le premier jour des applications complexes simplement en appuyant sur un bouton - le travail nécessaire pour une mise en œuvre «parfaite» dans toutes les applications est trop important.

C'est pourquoi une approche basée sur les risques est pertinente. Les principes suivants peuvent servir de critères d'évaluation: Si, dans une application,

- une grande quantité de données personnelles est traitée,
- données personnelles particulièrement sensibles sont traitées; et/ou
- il est procédé à des traitements divers et à haut risque des données;

les exigences concernant les mesures techniques et structurelles visant à garantir la sécurité des données sont d'autant plus élevées. Ces applications doivent donc être traitées en toute priorité.

Concept de solution technique

Il s'agit dès lors d'étudier et de concevoir pour l'application concernée la faisabilité technique de la suppression des données. Par expérience, il y a ici un certain retard à combler. Les systèmes sont plutôt conçus pour enregistrer, afficher et traiter des données. Mais pour ce qui est de supprimer ensuite les données définitivement et sous contrôle - il n'y a pas de «bouton» pour cela.

Les fabricants des applications sont ainsi invités y réfléchir: dans l'idéal, la suppression des données se fait via des procédures éprouvées avec des «Checks and Balances» et pas ad hoc par l'exécution d'un script directement sur une base de données. Il est dans tous les cas important que les dépendances entre les jeux de données soient prises en compte - pour que la suppression de données ne crée pas des cadavres de données.

Important: même si, par souci de pragmatisme, les banques se concentrent en général dans le premier cas d'application sur la clôture des relations clients, il faut aussi tenir compte de la suppression de certaines données personnelles à la demande du client, même pour une relation client en cours. Nous verrons à combien de telles demandes de suppression les banques seront confrontées dans les prochaines années. Selon notre expérience, les banques sont jusqu'à présent assez réticentes concernant la conception de mesures techniques et organisationnelles pour ces cas-là.

Mise en œuvre

En plus de l'implémentation technique de fonctionnalités de suppression et d'adaptations structurelles, deux autres aspects doivent être pris en compte:

1. Il apparaît souvent lors de l'analyse qu'un apurement des données personnelles dans les systèmes est nécessaire avant la suppression des données. Par exemple, les contrats sans date d'expiration ne peuvent pas être supprimés automatiquement. Il est donc important dans ce cas de saisir la date de suppression pour que le document puisse être supprimé automatiquement à l'issue du délai de conservation. L'expérience montre que de tels apurements des données peuvent générer beaucoup de travail. C'est pourquoi les activités de projet liées à la nLPD doivent commencer dès maintenant, même si l'entrée en vigueur ne devrait pas avoir lieu avant le milieu de l'année 2022.
2. La protection des données et la sécurité ne relèvent pas (seulement) du service informatique, mais sont l'affaire de la direction de l'entreprise. La direction doit avoir une conscience aiguë de ces questions. Mais pas seulement la direction. Pour minimiser le risque d'une infraction aux dispositions relatives à la protection des données, les collaborateurs doivent être sensibilisés et formés en permanence. La nLPD est donc une nouvelle occasion (nécessaire) de sensibiliser les collaborateurs à ce thème important.

Conclusion

Les conséquences de la révision de la loi sur la protection des données pour les banques ne doivent pas être sous-estimées: en plus de l'obligation de documentation (avec le registre des activités de traitement), des adaptations doivent être apportées aux applications bancaires et dans l'organisation de la banque. Il convient donc de s'emparer de ce sujet sans attendre.

Chez Swisscom, nous nous occupons depuis des années de la protection des données et des dispositions légales à ce sujet: que ce soit à cause de nos clients finaux Swisscom eux-mêmes, comme partenaire d'externalisation n°1 sur le marché bancaire suisse ou encore à travers le conseil aux banques sur le thème de la protection des données.

Notre équipe Conseil et Compliance a accompagné diverses banques: de l'interprétation de la nLPD à la mise en œuvre en passant par la conception. Nous vous accompagnerons volontiers - n'hésitez pas à nous contacter.

Sur l'auteur:

Silvan Lohri
Head Consulting Swisscom Banking
Silvan.Lohri@swisscom.com
+41 79 700 47 49
LinkedIn
Website

Août 2021 | Silvan Lohri, Head Consulting Swisscom Banking | Swisscom Business Customers