La nouvelle loi fédérale suisse sur la protection des données (nLPD): Ce que vous devez savoir

En bref

- La nLPD entre en vigueur le 1er septembre et remplace l'ancienne loi de 1992, sans délai de grâce pour le respect de la protection des données.
- Le consentement n'est pas requis pour la collecte/le traitement des données en toutes circonstances.
- La loi s'applique aux personnes physiques (et non plus aux personnes morales) et aux entités commerciales et non commerciales qui traitent les données de citoyens suisses.
- Les entités sont responsables du traitement conforme des données même si elles font appel à des tiers (comme des fournisseurs) pour le faire.
- Tous les sous-traitants doivent prendre des mesures organisationnelles et techniques raisonnables pour garantir la confidentialité et la sécurité des données.
- La loi s'applique aux données contenues dans des fichiers physiques et électroniques.
- C'est une loi extraterritoriale, les entités traitant des données personnelles n'ont pas besoin d'être situées en Suisse.
- Elle interdit les transferts de données personnelles de la Suisse vers des pays avec lesquels il n'existe pas d'accord d'adéquation, à moins que le consentement explicite n'ait été obtenu de la part des personnes concernées.

Exigences en matière de consentement

Contrairement au RGPD, la nLPD permet aux entités de traiter des données à caractère personnel sans consentement explicite, à moins que le traitement ne réponde à certains critères :

- traitement de données sensibles à caractère personnel,
- traitement utilisé dans le cadre d'un profilage à haut risque par une personne privée,
- traitement utilisé pour le profilage par un organe fédéral (gouvernement),
- les transferts de données vers des pays tiers où la protection des données n'est pas adéquate.

Outre le consentement, la nLPD autorise d'autres bases juridiques pour le traitement (comme la loi ou l'intérêt public supérieur), quoique moins nombreuses que celles prévues par le RGPD. Lorsque le consentement est requis, il doit être obtenu avant ou au moment de la collecte des données. Comme pour le RGPD, le consentement de l'utilisateur dans le cadre de la nLPD doit être granulaire, informé et volontaire.

Une plateforme de gestion du consentement permet de notifier l'utilisateur de manière conforme, en affichant par exemple une page de politique de confidentialité, ainsi que de collecter et de stocker des consentements conformes. Des configurations multiples peuvent être utilisées avec la géolocalisation pour assurer la conformité avec plusieurs réglementations ayant des exigences différentes, comme le RGPD et la nLPD, en fonction de la localisation de l'utilisateur.

Exigences en matière de notification

Les personnes concernées doivent systématiquement être informées avant la collecte des données, même si le consentement n'est pas requis pour le traitement des données envisagé.

Les entreprises doivent communiquer clairement les informations suivantes aux utilisateurs, par exemple sur une page du site web consacrée à la politique de confidentialité. Il s'agit des mêmes critères de notification que ceux requis pour que le consentement soit valide :

- l'identité du responsable du traitement des données, qu'il s'agisse de l'entreprise ou d'un tiers,
- les coordonnées du responsable du traitement,
- l'identité du destinataire des données et de toute autre partie ayant une quelconque implication avec le fichier de données,
- le pays destinataire si les données font l'objet d'un transfert transfrontalier,
- la ou les finalités de la collecte et de l'utilisation des données,
- les catégories de données collectées, le cas échéant,
- les moyens de collecte des données, le cas échéant,
- la base juridique du traitement, le cas échéant,
- les droits des utilisateurs concernant leurs données à caractère personnel en vertu de la nLPD, y compris le droit de refuser ou de retirer le consentement.

Droits des personnes concernées

En principe, une personne a les droits suivants :

- Droit d'accès : droit de demander des informations sur le traitement de ses données personnelles. Nul ne peut renoncer à l'avance au droit à l'information.
- Portabilité des données : droit d'obtenir les données dans un format électronique courant ou droit au transfert des données.
- Droit de rectification et d'effacement.

Check-list pour la mise en conformité avec la nLPD

- Rédiger des déclarations de confidentialité, telle qu'une page de politique de confidentialité sur le site web, ou mettre à jour les déclarations existantes et s'assurer qu'elles sont adaptées à votre entreprise, à vos utilisateurs, à la finalité du traitement et aux données que vous traitez.
  - Les personnes concernées doivent toujours être informées du traitement de leurs données, même si leur consentement n'est pas requis.
  - Une plateforme de gestion des consentements permet de personnaliser et d'alimenter votre politique de confidentialité, ainsi que de la tenir à jour.
- Veillez à ce que les informations de notification précisent les pays avec lesquels les données personnelles sont partagées.
  - S'il n'existe pas d'accord d'adéquation avec ces pays, indiquez-le clairement et obtenez un consentement explicite pour le partage des données.
- Obtenir et conserver en toute sécurité le consentement de l'utilisateur lorsque cela est nécessaire, par exemple pour le traitement de données personnelles sensibles.
- Créer ou mettre à jour des directives internes en matière de traitement des données et veiller à ce qu'elles soient bien communiquées.
- Mettre en place et tenir à jour un registre interne des activités de traitement des données.
- Mettre en œuvre une procédure permettant de recevoir, d'accuser réception et de répondre efficacement aux personnes concernées qui exercent leurs droits, par exemple les demandes de copies de données à caractère personnel, de rectification ou d'effacement.
  - Veiller à ce que les données soient portables dans un format accessible, par exemple une impression ou un format électronique courant.
- Mettre en œuvre une évaluation de l'impact de la protection des données, surtout si l'organisation traite de manière extensive des données sensibles.
- Mettre en place une procédure en cas de fuite de données, comprenant notification rapide au PFPDT et aux personnes concernées si nécessaire. Inclure également les tiers qui accèdent aux données ou les traitent.
- Réviser et mettre à jour les contrats avec le responsable du traitement des données (comme les fournisseurs) pour s'assurer que les exigences raisonnables en matière de sécurité et de confidentialité des données sont respectées. (Bien que la responsabilité juridique incombe à celui-ci).
- Conserver les données uniquement pendant la durée nécessaire prévue par la notification, et pour la finalité du traitement mentionnée. Supprimez-les ou rendez-les anonymes dès qu'elles ne sont plus nécessaires à cette finalité.
- Désigner un délégué à la protection des données qui assurera la liaison avec les utilisateurs et le PFPDT, et qui gérera les politiques et les processus, si cela est nécessaire pour votre entreprise.
- Consultez un conseiller juridique qualifié au sujet des responsabilités de votre organisation en vertu de la nLPD et des modalités de leur mise en œuvre. Webrepublic et Usercentrics ne fournissent pas de conseils juridiques mais seulement des informations à des fins didactiques.

web republic × usercentrics