BIANCHISCHWALD

NEWS

NOUVELLE LOI FÉDÉRALE SUR LA PROTECTION DES DONNÉES POUR LA SUISSE

Le 25 septembre 2020, le Parlement suisse a adopté la loi fédérale sur la protection des données révisée (« nLPD »). L'entrée en vigueur de cette nouvelle loi est encore incertaine mais devrait intervenir au plus tôt dans la seconde moitié de 2021. Comme la nLPD ne prévoit pas de période transitoire, il est conseillé de commencer les adaptations en temps utile.

Un objectif important de la révision était d'assurer un niveau de protection équivalent à celui offert par le Règlement général sur la protection des données de l'UE (« RGPD »). Cela est nécessaire pour que la Suisse puisse continuer à bénéficier des avantages de la décision d'adéquation de la Commission européenne. Si un niveau de protection équivalent à celui de l'UE n'est plus reconnu, les données personnelles provenant de l'Espace économique européen (« EEE ») ne pourraient être transférées en Suisse qu'avec des mesures de sécurité supplémentaires. Il n'a pas encore été communiqué quand est-ce que la Commission européenne prendra sa décision sur l'adéquation du nLPD.

QU'EST-CE QUI CHANGE ?

La révision n'entraîne pas d'exigences fondamentalement différentes pour le traitement des données personnelles. Ce qui reste inchangé, c'est que le traitement des données est en principe autorisé pour les entreprises privées et qu'une justification (comme par exemple le consentement de la personne concernée) n'est requise que dans le cas d'une atteinte aux droits de la personnalité. Néanmoins, de nombreuses nouveautés doivent être observées et mises en pratique. Ci-après vous trouvez un aperçu des changements importants qui sont significatifs pour un grand nombre d'entreprises. La nLPD entraîne également des changements dans le traitement des données personnelles par les organes fédéraux. Ces changements ne sont pas présentés ci-après.

RÉPERTOIRE DES ACTIVITÉS DE TRAITEMENT DES DONNÉES

Nouvellement, lors du traitement des données personnelles, le responsable du traitement des données devra tenir un répertoire des activités de traitement des données. La même obligation s'applique aux sous-traitants qui traitent des données personnelles pour le compte du responsable. Le contenu minimum de ces répertoires est prescrit par la loi et comprend, par exemple, l'identité du responsable du traitement des données, le but du traitement des données, les catégories des personnes concernées et les catégories de données personnelles traitées. Le Conseil fédéral peut prévoir des exceptions pour les PME de moins de 250 employés dont le traitement des données personnelles comporte un faible risque de violation des données personnelles. Le projet d'ordonnance réglementant ces exceptions n'est pas encore disponible. Il n'est donc pas encore clair dans quelle mesure les entreprises seront effectivement exemptées de cette obligation administrative. Dans tous les cas, il est difficile de respecter la réglementation en matière de protection des données sans avoir une vue d'ensemble rudimentaire des opérations de traitement des données.

AMPLIFICATION DE L'OBLIGATION D'INFORMATION

Le nLPD prévoit expressément une obligation d'information dans le cadre du traitement des données personnelles. Des informations suffisantes doivent être mises à la disposition des personnes concernées afin de garantir un traitement transparent des données et ainsi garantir leurs droits. Cette obligation d'information comprend au moins l'identité et les coordonnées de la personne responsable, ainsi que la but du traitement pour lequel les données personnelles sont obtenues. Si les données personnelles sont divulguées à des tiers ou transférées à l'étranger, des informations complémentaires sont nécessaires. La violation de cette obligation peut avoir des conséquences pénales.

OBLIGATION DE DÉCLARER LES VIOLATIONS DE LA PROTECTION DES DONNÉES

Dans le cas où une violation de la protection des données entraîne un risque élevé pour la personne concernée (par exemple une violation des droits de la personnalité ou des droits fondamentaux), le Préposé fédéral à la protection des données et à la transparence («PFPDT») doit en être informé. Une violation de la protection des données se produit notamment lorsque des données personnelles sont accidentellement perdues, détruites ou altérées,

ou deviennent accessibles à des personnes non autorisées. La loi ne fixe pas de date limite pour cette déclaration, mais elle stipule que cette dernière doit avoir lieu le plus tôt possible. Le contenu minimum de cette déclaration est prescrit par la loi : doivent être communiqués en particulier le type de violation de la protection des données, ses conséquences et les mesures prises ou prévues.

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Le responsable du traitement des données doit établir une analyse d'impact relative à la protection des données («AIPD») lorsqu'un traitement des données prévu pourrait entraîner un risque élevé de violation des droits de la personnalité ou des droits fondamentaux. Un risque élevé existe notamment lorsque de nouvelles technologies sont utilisées, lorsque des données personnelles particulièrement sensibles (comme par exemple les données sur la santé) sont traitées de manière extensive (comme par exemple dans le cadre d'un projet de recherche médicale) ou lorsque de vastes espaces publics sont systématiquement surveillés (comme par exemple le hall d'une gare). Outre une description du traitement des données prévu, l'AIPD doit contenir une évaluation des risques et les mesures de protection prévues. Si élevé malgré les mesures de protection, il réside un risque élevé pour le traitement des données prévu, il doit être soumis au PFPDT. Si le PFPDT soulève des objections au traitement des données prévu, il propose des mesures de protection appropriées à la personne responsable. Étant donné que le PFPDT dispose de deux mois (voire trois mois en cas de traitement complexe) pour répondre, il est conseillé de soumettre le cas au PFPDT rapidement.

REPRÉSENTANT EN SUISSE

Sous certaines conditions, la nLDN prévoit l'obligation pour les entreprises étrangères de désigner un représentant en Suisse. La représentation sert de point de contact pour les personnes concernées et le PFPDT. Toutefois, l'obligation n'existe que si plusieurs conditions cumulatives sont remplies : l'entreprise étrangère doit être orientée vers la Suisse et, dans ce contexte, doit traiter les données personnelles de manière régulière et complète. En même temps, le traitement doit comporter un risque élevé de violation des droits de la personne ou des droits fondamentaux. Ces conditions (et l'obligation de désigner un représentant qui y est associée) ne seront satisfaites que dans des cas individuels.

DROITS DE LA PERSONNE CONCERNÉE

Le nLPD prévoit des droits supplémentaires pour les personnes concernées. Il convient de mentionner en particulier le droit à la production et à la transmission de données (aussi appelée « la portabilité des données ») ainsi que le devoir d'information dans le cas de décisions individuelles automatisées. Le droit à la portabilité des données permet à la personne concernée de demander au responsable du traitement des données de lui communiquer gratuitement ses données personnelles (données qu'elle a communiquées au responsable du traitement des données) dans un format courant (lisible en machine). La personne concernée peut également demander que ses données personnelles soient transférées à un autre responsable. Cela suppose que le responsable du traitement des données traite les données par des moyens automatisés (c'est-à-dire non analogues) et que les données personnelles sont traitées en relation directe avec un contrat avec la personne concernée ou sur la base du consentement de cette dernière. Les scénarios d'application possibles de cette disposition sont, par exemple, un changement de banque ou de compagnie d'assurance. La personne concernée peut demander que les données personnelles existantes soient transférées directement au nouveau prestataire de services. Pour l'entreprise, ce droit signifie que les conditions techniques préalables à l'exercice de ce droit doivent être créées.

En outre, une obligation d'information est nouvellement prescrite pour les décisions fondées exclusivement sur le traitement automatisé des données personnelles. Le responsable du traitement des données doit informer la personne concernée si la décision est susceptible d'affecter de manière significative la personne concernée ou si la décision «entraîne une conséquence juridique». Une telle conséquence juridique est notamment la conclusion ou la résiliation d'un contrat. Il est à prévoir que le PFPDT publiera des lignes directrices ou des fiches d'information afin de clarifier ces termes juridiques non définis. En attendant que ces lignes directrices soient communiquées, il est conseillé d'informer les personnes concernées en cas de doute.

MISE EN ŒUVRE ET SANCTIONS

Afin de garantir le respect des obligations en matière de protection des données, les sanctions pénales ont été considérablement renforcées. Les violations des règles en matière de protection des données pourront à l'avenir être sanctionnées par des amendes allant jusqu'à 250'000 francs suisses (comparé à 10'000 francs suisses auparavant). La responsabilité pénale est dirigée contre la personne physique qui commet la violation. Les organes exécutifs des entreprises qui, intentionnellement ou par négligence, ne mettent pas fin à la violation, en violation d'une obligation légale, peuvent également être tenus pénalement responsables. De même, la personne morale peut même être sanctionnée d'une amende dans certains cas. Les cantons sont responsables des poursuites pénales.

Parallèlement, le PFPDT reçoit de nouvelles compétences. Sa sphère d'influence ne sera plus limitée à quelques domaines, mais il pourra agir dans tous les cas de violation de la protection des données. En outre, le PFPDT pourra à l'avenir édicter des décrets contraignants et ordonner aux responsables d'adapter ou d'arrêter le traitement de données et de supprimer les données personnelles concernées. Le non-respect délibéré des ordres du PFPDT peut faire l'objet de poursuites pénales.

QUE FAUT-IL FAIRE ?

La nécessité d'agir pour mettre en œuvre la nLPD est moindre pour les entreprises qui se conforment déjà aux exigences du RGDP. Si tel est le cas, les conditions cadres internes en matière de protection des données existantes peuvent être simplement adaptées aux particularités da la nLPD, ce qui nécessite que certaines modifications ponctuelles. Les entreprises étrangères doivent vérifier si un bureau de représentation en Suisse doit être désigné. Si un tel cadre n'a pas encore été mis en place (ou si un réexamen périodique est de toute façon prévu), la première étape consiste à vérifier quelles données personnelles sont traitées de quelle manière dans l'entreprise (aussi appelé « Data Mapping »). Les données personnelles sont toutes les informations qui se rapportent à une personne physique identifiée ou identifiable. Ce terme inclut donc, par exemple, les informations sur les employés, les clients et les personnes de contact chez les fournisseurs ainsi que les visiteurs du site internet. Contrairement à la loi actuelle sur la protection des données, les données personnelles des personnes morales ne seront plus couvertes par le nLPD.

Les résultats du «Data Mapping» doivent être présentés dans une vue d'ensemble (le répertoire des activités de traitement), vérifiés périodiquement et ajustés si nécessaire. Sur la base de cet aperçu, il faut également vérifier si tous les documents requis ont été établis et les processus requis documentés. Il faut tout au moins vérifier les aspects suivants :

- Les sous-traitants qui ont été chargés par le responsable du traitement des données personnelles (existe-t-il des contrats écrits ? répondent-ils aux exigences de la nLPD?)

- Les transferts de données à l'étranger (les transferts vers des pays n'ayant pas un niveau de protection suffisant ne sont-ils effectués qu'avec les mesures de protection appropriées ?)

- La déclaration de protection des données (tous les traitements de données personnels sont-ils couverts ? Les informations répondent-elles aux exigences minimales de la nLPD) ?

- Existe-t-il un processus permettant de remplir l'obligation de déclarer les violations de la protection des données ?

- Existe-t-il un processus permettant la réalisation d'analyses d'impact relatives à la protection des données ?

- Est-il garanti que les demandes des personnes concernées sont traitées en temps utile et de manière complète ?

CHRISTOPH GASSER
Avocat, Dr. iur.,
LL.M. University of Michigan
Juge à temps partiel au
Tribunal fédéral des brevets
Associé | Zurich

THIERRY BURNENS
Avocat, M.A. HSG, CIPP/E
Collaborateur | Zurich

STEPHANIE VOLZ
Avocate, Dr. iur.
Collaboratrice | Zurich

LINDA CETKOVIC
LL.M. Maastricht University
Avocate stagiaire | Lausanne

BIANCHISCHWALD SÀRL
mail@bianchischwald.ch
bianchischwald.ch

GENÈVE
5, rue Jacques-Balmat
Case postale 5839
CH-1211 Genève 11
T +41 58 220 36 00
F +41 58 220 36 01

ZURICH
St. Annagasse 9
Case postale 1162
CH-8021 Zurich
T +41 58 220 37 00
F +41 58 220 37 01

LAUSANNE
12, avenue des Toises
Case postale 5410
CH-1002 Lausanne
T +41 58 220 36 70
F +41 58 220 36 71

BERNE
Elfenstrasse 19
Case postale 1208
3000 Berne 16
T +41 58 220 37 70
F +41 58 220 37 71