Monthly
Newsletter
December 2022

Data

Mise en œuvre de la nouvelle Loi sur la protection des données : Étape 3

Samuel Klaus, Roland Mathys, Kenzo Thomann

Key Take-aways

1.
Le registre des traitements avec l'aperçu des traitements de données peut servir de point de départ pour la mise en œuvre des différentes mesures.

2.
Un règlement interne général sur la protection des données est conseillé. Dans certains cas un règlement de traitement spécifique peut être obligatoire et les employés doivent être formés en conséquence.

3.
Les responsabilités, processus et modèles doivent être définis pour les analyses d'impact sur la protection des données, les annonces de violations et les décisions individuelles automatisées.

1 Aperçu

La nouvelle Loi fédérale sur la protection des données (**nLPD**) et la nouvelle Ordonnance sur la protection des données (**OPDo**) entreront en vigueur le 1er septembre 2023. Dans notre newsletter d'octobre 2022, nous avons présenté un plan de **mise en œuvre** en trois étapes et décrit la première étape (préparation). L'étape 2 se concentre sur les mesures à effet externe et a été traitée dans la newsletter de novembre 2022. Avec **l'étape 3**, nous examinons maintenant les mesures à effet interne :

- **Contrats et règlements** (sous-traitance, devoir de discrétion, règlement de protection des données et formations)
- **Processus opérationnels** (analyse d'impact sur la protection des données, obligation d'annonce des violations de la sécurité des données, décisions individuelles automatisées)
- **Processus administratifs / techniques** (registre de traitement, portabilité des données, durée de conservation)

2 Contrats et règlements

2.1 Sous-traitance

Lorsque le responsable (*controller*) fait effectuer certains traitements par un sous-traitant (*processor*), la nLPD prévoit désormais des exigences plus strictes : le **contrat de traitement des données** (*Data Processing Agreement*, **DPA**) doit garantir que le *processor* ne traite les données que comme le *controller* pourrait le faire lui-même et qu'il ne fasse pas appel à des sous-traitants (*sub-processors*) sans l'autorisation du *controller*. Il convient de prévoir à cet effet des droits d'instruction et de contrôle ainsi que des mécanismes d'approbation. Les modèles élaborés pour la mise en œuvre de l'art. 28 du règlement général sur la protection des données (**RGPD**) de l'UE satisfont aux exigences de la nLPD, à condition que leur formulation soit adaptée au droit suisse.

La sous-traitance intra-groupe est également prise en compte et une partie des obligations relatives à la sous-traitance **est désormais punissable** sous la nLPD. Les DPA existants doivent être examinés et le respect des exigences minimales doit être garanti pour les nouveaux DPA.

2.2 Devoir de discrétion

La loi en vigueur punit déjà la **violation du devoir de discrétion**, mais de façon limitée aux données personnelles secrètes sensibles et aux profils de la personnalité (art. 35 LPD). Sous la nLPD, **toutes les données personnelles secrètes** seront couvertes : ce n'est donc plus le type de données qui est important, mais uniquement le fait qu'il s'agisse de données "secrètes" : il faut que la personne concernée ait un intérêt (reconnaissable) à garder le secret et la volonté de le garder, et que les données ne soient pas déjà connues de tous (ou accessibles). Quiconque révèle intentionnellement des données personnelles secrètes peut être puni d'une **amende allant jusqu'à CHF 250'000** sous la nLPD.

Si des données personnelles secrètes sont traitées, il convient d'examiner si une **réglementation doit être prévue dans les contrats avec les clients** (ou avec d'autres personnes concernées, dans les conditions générales, etc.). Dans tous les cas, il est conseillé d'établir des directives internes à ce sujet et de sensibiliser les collaborateurs.

2.3 Règlement sur la protection des données et formations

Contrairement au RGPD, la nLPD ne prévoit pas d'obligation générale de rendre des comptes. Pour **garantir la sécurité des données**, il faut toutefois prendre des mesures techniques et organisationnelles (**TOM**) appropriées et les documenter. L'OPDo contient à ce sujet d'autres prescriptions, y compris **l'obligation d'établir un règlement de traitement** : si des données personnelles sensibles sont traitées à grande échelle de manière automatisée ou si un profilage à risque élevé est effectué de manière automatisée, un règlement de traitement doit être établi avec le **contenu minimal prévu à l'art. 5 OPDo**. Le non-respect intentionnel des prescriptions relatives aux exigences minimales peut être sanctionné par une **amende pouvant atteindre CHF 250'000**.

Même si on ne doit pas établir un règlement de traitement spécial, un **règlement général de protection des données** est recommandé pour la mise en œuvre des TOM, qui précise comment les données personnelles sont traitées au sein de l'entreprise, quelles sont les compétences, etc. Ces directives doivent être effectivement appliquées : les collaborateurs doivent être rendus attentifs à leurs obligations par le biais de **formations et d'entraînements** appropriés et être soutenus dans leur mise en œuvre. Il est également conseillé de les sensibiliser à l'extension du devoir de discrétion (voir ci-dessus).

La sous-traitance de traitement de données nécessite des mesures contractuelles.

3 Processus opérationnels

3.1 Analyse d'impact relative à la protection des données personnelles (AIPD)

Si un nouveau traitement de données est prévu et qu'il peut entraîner un risque élevé pour la personne concernée, une **analyse d'impact relative à la protection des données (AIPD)** doit être effectuée. Un risque élevé peut résulter de la nature, de la portée, des circonstances et de la finalité du traitement des données, notamment de l'utilisation de nouvelles technologies (telles que l'intelligence artificielle, **IA**). L'AIPD sert à évaluer les risques y relatifs et à mettre en œuvre des mesures de réduction des risques (comme la minimisation des données, l'anonymisation, les restrictions d'accès, etc.)

L'étendue et le niveau de détail de l'AIPD dépendent de la complexité et du profil de risque du traitement prévu. Pour l'AIPD, les représentants opérationnels doivent travailler en étroite collaboration avec les représentants du service juridique/compliance. Si l'AIPD aboutit à la conclusion que les mesures prévues ne permettent pas de limiter suffisamment

le risque, le Préposé fédéral à la protection des données et à la transparence (**PFPDT**) (ou le conseiller à la protection des données interne, s'il en a été nommé un) doit être consulté avant la mise en œuvre du traitement de données prévu.

Dans certaines circonstances, un règlement de traitement spécial doit être établi.

3.2 Obligation d'annoncer les violations de la sécurité des données

La nLPD introduit désormais **l'obligation d'annoncer les violations de la sécurité des données**. En cas de violation de la sécurité des données (p. ex. perte de données, que ce soit sur papier ou sous forme numérique, accès non autorisé, etc.), le **PFPDT** doit être informé si cette violation est susceptible d'entraîner un risque élevé pour les personnes concernées. La nLPD ne prévoit pas de délai précis pour l'annonce ; celle-ci doit toutefois être effectuée **le plus rapidement possible**, en s'inspirant du délai de 72 heures prévu par le RGPD. **Les personnes concernées** doivent être informées lorsque cela est nécessaire pour leur protection (p. ex. parce que les cartes de crédit doivent être bloquées ou les mots de passe changés) ou lorsque le PFPDT l'exige.

Pour la mise en œuvre, il convient de définir les **compétences et les processus** afin de savoir clairement qui prend quelles décisions et selon quels critères dans la période de stress qui suit immédiatement la découverte d'une violation de la sécurité des données. La violation de l'obligation d'annonce n'est certes pas punissable (contrairement au RGPD), mais peut nuire à la réputation de l'entreprise (et éventuellement déclencher une enquête du PFPDT).

Il convient de tenir compte **d'autres obligations d'annonce légales ou contractuelles** et il n'est souvent pas clair à l'égard de quelles parties contractantes une telle obligation existe. Il convient donc d'établir (et de tenir à jour) un aperçu séparé de ces obligations d'annonce, notamment pour éviter les conséquences contractuelles en matière de responsabilité.

3.3 Décisions individuelles automatisées

Les décisions individuelles automatisées (DIA) sont des décisions discrétionnaires prises par l'IA sans intervention humaine et qui ont un impact pertinent sur les personnes concernées : p. ex. l'affichage automatique d'une publicité personnalisée sur un site web n'est pas une DIA, alors que le tri d'une candidature d'emploi basé uniquement sur l'IA l'est.

Si des DIA sont utilisées, des exigences supplémentaires concernant **l'obligation d'information** ou la **déclaration de protection des données** doivent être respectées et des **processus spéciaux de consultation et de contrôle** doivent être prévus. Ces obligations sont parfois assorties de **sanctions pénales**. L'utilisation de DIA devrait donc être identifiée et abordée à un stade précoce (p. ex. si de nouveaux logiciels dotés de fonctions DIA sont mis en œuvre).

4 Processus administratifs / techniques

4.1 Registre des activités de traitement

Nous avons déjà souligné l'importance du **registre des traitements** dans notre newsletter d'octobre 2022, car c'est **l'instrument central de la mise en œuvre de la nLPD** qui sert de point de départ à toutes les mesures. Tant le responsable (*controller*) que le sous-traitant (*processor*) doivent en principe tenir un registre, l'art. 12 nLPD fixant pour chacun d'eux des prescriptions différentes quant au contenu minimal.

En revanche, il n'existe pas de prescriptions concernant la **forme et la structure**. Il est possible d'utiliser des solutions logicielles répandues sur le marché ou - surtout pour les situations simples - de créer soi-même un registre (p. ex. dans Word ou Excel). Il est utile que la structure s'oriente vers **les traitements de données effectués**, car cela facilite l'utilisation directe des informations pour d'autres mesures. Si la structure s'oriente plus vers les aspects techniques, cela peut rendre difficile la réutilisation de ces informations pour les autres mesures.

Les nouveaux traitements de données à haut risque doivent faire l'objet d'une AIPD.

4.2 Portabilité des données

Concernant la **portabilité des données**, le responsable doit remettre aux personnes concernées les données personnelles traitées de manière automatisée **qu'elles lui ont elles-mêmes communiquées** ou que le responsable a collectées à leur sujet **lors de l'utilisation d'un service ou d'un appareil** (p. ex. un traqueur de fitness). Les données que le responsable a lui-même générées à partir des données collectées en les analysant lui-même (p. ex. le profil individuel de l'utilisateur créé à partir des données collectées) ne doivent pas être remis. Les données doivent être fournies dans un **format électronique courant**.

Pour qu'une telle remise soit possible, il faut s'assurer que les données d'une personne concernée puissent être **identifiées**, **isolées** des autres données et, si nécessaire, **migrées** dans un format électronique courant.

4.3 Période de conservation

Il découle du **principe de minimisation des données** que celles-ci **doivent être effacées** lorsqu'elles ne sont plus nécessaires à la finalité initiale. Les exceptions à cette règle doivent être justifiées, par exemple en raison de dispositions légales ou contractuelles relatives à la conservation des données ou d'un intérêt prépondérant du responsable du traite-

ment (p. ex. tant que les données peuvent encore être utilisées dans le cadre d'un éventuel litige).

La mise en œuvre devrait se faire par l'élaboration d'un **règlement de conservation** définissant la durée de conservation par catégorie de données et les étapes nécessaires à l'effacement. Dans ce contexte, les **processus d'effacement** doivent également être mis en œuvre (p. ex. en fixant une "date d'expiration" pour les données) et réellement appliqués (p. ex. par des routines annuelles d'archivage et effacement).

5 Conclusion et perspectives

C'est précisément dans le domaine des mesures avec effets internes que la nLPD apporte de **nouvelles obligations importantes** qui ne devraient pas être sous-estimées. Leur mise en œuvre n'est en soi pas si complexe, mais implique un effort certain et doit être soigneusement planifiée et lancée rapidement.

Nous avons traité le plan de mise en œuvre dans la newsletter d'octobre 2022 et les mesures à effet externe dans la newsletter de novembre 2022. Cette newsletter sur les mesures à effet interne clôt notre série en trois parties sur la mise en œuvre de la nLPD.

Vincent Carron
Associé Genève
vincent.carron@swlegal.ch

Dr. Catherine Weniger
Conseil Genève
catherine.weniger@swlegal.ch

Roland Mathys
Associé Zurich
roland.mathys@swlegal.ch

Dr. Samuel Klaus
Associé Zurich
samuel.klaus@swlegal.ch

Schellenberg Wittmer SA
Avocats

Zurich
Löwenstrasse 19
Case postale 2201
8021 Zurich / Suisse
T +41 44 215 5252
www.swlegal.com

Genève
15bis, rue des Alpes
Case postale 2088
1211 Genève 1 / Suisse
T +41 22 707 8000
www.swlegal.com

Singapour
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapour 049909
T +65 6580 2240
www.swlegal.sg