Frôté & Partner
AVOCATS & NOTAIRES
RECHTSANWÄLTE & NOTARE

Nouvelle Loi sur la protection des données dès le 1er septembre 2023

La réglementation concernant la protection des données en Suisse va changer à l'automne avec l'entrée en vigueur le 1er septembre 2023 de la nouvelle Loi fédérale sur la protection des données.

La nouvelle loi remplacera la loi actuelle qui date de 1992. Face à la forte évolution numérique elle renforce et adapte la protection des données et harmonise le droit suisse avec le droit européen.

Les nouvelles dispositions instaurent davantage de transparence sur les données personnelles collectées et leur traitement, et confèrent des droits aux personnes concernées, qui pourront dorénavant avoir une meilleure maîtrise de ces données.

Le nouveau droit s'aligne sur les standards de protection européens et donne ainsi à la Suisse le statut d'état offrant un niveau de protection des données adéquat au sens du droit de l'Union européenne, permettant des échanges de données avec l'UE sans exigences supplémentaires, favorisant ainsi la compétitivité de l'économie suisse. Sans cette équivalence, les entreprises auraient été contraintes de prouver au cas par cas qu'elles garantissent la protection des données.

La loi qui entrera en vigueur remodèle en profondeur la règlementation sur la protection des données. L'objet des présentes lignes n'est pas une présentation exhaustive de la nouvelle loi, mais bien plutôt la mise en évidence de quelques éléments choisis qui feront partie de notre paysage juridique dès le mois de septembre.

1. Focus sur quelques éléments choisis

1.1. Quelques définitions et champ d'application

Les données personnelles englobent toutes les informations concernant une personne physique identifiée ou identifiable. La nouvelle Loi sur la protection des données (nLPD) s'applique uniquement au traitement de données personnelles de personnes physiques, à l'exclusion de celles de personnes morales.[1]
Elle ne s'applique pas non plus au traitement de données personnelles par une personne physique pour un usage uniquement personnel.

La nLPD s'applique en Suisse, mais peut également s'appliquer à des personnes physiques situées en dehors de la Suisse : un état de fait qui s'est produit à l'étranger est soumis à la nLPD s'il déploie des effets en Suisse[2].

[1] Art. 2 nLPD
[2] art. 3 nLPD

Toute opération effectuée en relation avec des données personnelles constitue un « traitement » de ces données : notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction des données[3] .

Le responsable du traitement peut confier le traitement de données personnelles à un sous-traitant si un contrat ou la loi le prévoit, si le sous-traitant n'effectue que les traitements que le responsable du traitement serait en droit d'effectuer lui-même et si aucune obligation légale ou contractuelle de garder le secret ne l'interdit.[4]

1.2. Devoir d'information et consentement

Les personnes concernées doivent être informées[5] que leurs données personnelles sont collectées et des traitements dont celle-ci font l'objet ainsi que de la finalité de ce traitement. Cette information pourra se faire par exemple par le biais d'une déclaration de confidentialité, qui sera transmise ou signalée aux personnes concernées. Le devoir d'information en cas de décisions individuelles automatisées est réglé de manière spécifique[6] .

Un consentement exprès de la personne concernée est requis dans les 3 cas suivants[7] :

- En cas de traitement de données sensibles : les données dites « sensibles » sont celles qui concernent les opinions ou activités religieuses, philosophiques, politiques ou syndicale ; la santé, la sphère intime ou l'origine raciale ou ethnique ; les données génétiques ; les données biométriques ; les données sur des poursuites ou des sanctions pénales ou administratives ; les données sur des mesures d'aide sociale.
- En cas de profilage à risque élevée effectuée par une personne privée : Aujourd'hui les données de mouvements permettent de voir qui rencontre qui, à quel moment, à quelle heure et à quel endroit. Ces renseignements méritent une protection particulière. Le traitement de données permettant de dresser un profil précis de la personnalité des personnes grâce à un appariement des données provenant de sources différentes est strictement encadré, et notamment le consentement exprès de la personne concernée est exigé.
- En cas de profilage effectué par un organe fédéral.

Exceptions au devoir d'informer [8] :

- Lorsque la personne concernée possède déjà les informations correspondantes ;
- lorsque le traitement des données est prévu par la loi ;
- lorsque le responsable du traitement est une personne privée liée par une obligation légale de garder le secret ;
- lorsque les données sont traitées pour la publication dans un médias, aux conditions posées à l'art 27 nLPD.

[3] art. 5 let. d nLPD
[4] art. 9 nLPD
[5] art. 19 nLPD
[6] art. 21 nLPD
[7] art. 7 ch. 7 nLPD
[8] art. 20 nLPD

Quand les données ne sont pas récoltées auprès de la personne concernée, le devoir d'information ne s'applique pas si l'information est impossible à donner ou nécessite des efforts disproportionnés.

Enfin le responsable du traitement peut restreindre, différer ou renoncer à la communication des informations notamment si des intérêts prépondérants d'un tiers l'exigent ou si l'information empêche le traitement d'atteindre son but[9].

1.3. Principe de sécurité

Le responsable du traitement doit prendre les mesures techniques (par ex : authentification par un mot de passe, chiffrement des données, sauvegardes régulières, etc) et organisationnelles (par ex : formation, instructions, contrôles, etc) nécessaires pour effectuer un traitement sûr et éviter toute violation de la sécurité des données.[10]

Devoir d'annoncer les violations [11]: Les violations de la sécurité des données qui entraînent vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne doivent être annoncées dans les meilleurs délais au Préposé fédéral à la protection des données (PFPDT)[12]. C'est le cas, par exemple, quand la violation peut engendrer des dommages physiques, matériels ou un préjudice moral pour les personnes dont les données ont fait l'objet de la violation.
La violation doit être communiquée en plus à la personne concernée quand c'est nécessaire à sa protection ou quand le PFPDT l'exige.

1.4. Droit d'accès

La personne concernée a dorénavant un droit d'accès aux données personnelles la concernant. La loi précise les informations qui doivent être communiquées à la personne qui exerce son droit d'accès afin qu'elle puisse faire valoir ses droits et que la transparence soit respectée[13].

1.5. Obligation de tenir un registre des traitements

Le responsable de traitement (et le sous-traitant) a l'obligation de tenir un registre des activités de traitement[14]. Des exceptions sont prévues pour les personnes physiques et les entreprises qui emploient moins de 250 employés, dont le traitement ne porte pas sur des données sensibles à grande échelle ou ne constitue pas un profilage à risque élevé[15] .

1.6. Renforcement des sanctions pénales[16]

Les sanctions pénales iront jusqu'à CHF 250'000.— (actuellement CHF 10'000.--). Les sanctions viseront non pas l'entreprise, mais la personne physique responsable (membres du conseil d'administration et/ou de la direction).

---

[9] art. 20 al. 3 nLPD
[10] art. 8 nLPD
[11] art. 24 al. 4 nLPD
[12] art. 24 nLPD
[13] art. 25 nLPD
[14] art. 12 nLPD
[15] art. 24 nOrdonnance sur la protection des données (OPDo)
[16] art. 60ss nLPD

2. Conclusions

La nouvelle loi sur la protection des données amène de nombreux changements, de nouvelles obligations et des exigences accrues en matière de protection des données.

Cette mise à jour profonde de la loi rend nécessaire un exercice d'introspection auquel les entreprises suisses ont encore quelques mois pour se livrer, afin de déterminer leur niveau actuel de conformité en matière de protection des données, et surtout pour mettre en place les différentes mesures et processus qui leur permettront de garantir une protection optimale et conforme des données.

Neuchâtel, Etude Frôté & Partner, Rachel Gagnebin D'Onofrio, le 2 février 2023

Frôté & Partner
AVOCATS & NOTAIRES
RECHTSANWÄLTE & NOTARE

Neues Datenschutzgesetz ab dem 1. September 2023

Die Regelung des Datenschutzes in der Schweiz wird sich im Herbst mit dem Inkrafttreten des neuen Bundesgesetzes über den Datenschutz am 01. September 2023 ändern.

Das neue Gesetz wird an die Stelle des bisherigen, aus dem Jahr 1992 stammenden Gesetzes treten. Das Gesetz ist darauf ausgerichtet, angesichts der massiven Digitalisierung, den Schutz der Daten zu stärken und anzupassen und das Schweizer Recht an EU-Recht anzugleichen.

Die neuen Bestimmungen sorgen für mehr Transparenz, was die erfassten personenbezogenen Daten und ihre Bearbeitung anbelangt, und sie räumen betroffenen Personen Rechte ein, die ihnen mehr Selbstbestimmung hinsichtlich ihrer Daten verschaffen.

Das neue Recht stützt sich auf die europäischen Schutzstandards und überträgt der Schweiz damit den Status eines Staates mit angemessenem Schutzniveau im Sinne des EU-Rechts. Dadurch ist der Datenaustausch mit der EU ohne zusätzliche Anforderungen möglich, was der Wettbewerbsfähigkeit der Schweizer Wirtschaft den Rücken stärken dürfte. Ohne diese Gleichwertigkeit wären die Unternehmen gezwungen, bei jedem Datenaustausch nachzuweisen, dass sie den Schutz der Daten garantieren.

Das neue Gesetz ist eine Totalrevision der derzeit geltenden Datenschutzbestimmungen. Mit den nachfolgenden Ausführungen möchten wir nicht das neue Gesetz mit all seinen Facetten vorstellen, sondern vielmehr einige Neuerungen hervorheben, die ab September geltendes Recht sein werden.

1. Einige Neuerungen im Fokus

1.1. Begriffserklärungen und Geltungsbereich

Als personenbezogene Daten gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Das neue Bundesgesetz über den Datenschutz (nDSG) bezieht sich nur noch auf die Bearbeitung personenbezogener Daten von natürlichen Personen, und nicht auf diejenigen von juristischen Personen.[1]
Es gilt ebenfalls nicht für die Bearbeitung personenbezogener Daten durch eine natürliche Person zum ausschliesslich persönlichen Gebrauch.

Das nDSG gilt in der Schweiz, kann jedoch auch natürliche Personen ausserhalb der Schweiz betreffen: ein Sachverhalt, der im Ausland veranlasst wird, unterliegt dann dem nDSG, wenn er sich in der Schweiz auswirkt[2].

[1] Artikel 2 nDSG
[2] Artikel 3 nDSG

Jeder Umgang mit personenbezogenen Daten stellt eine „Bearbeitung“ dieser Daten dar, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten[3].

Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte und wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.[4]

1.2. Informationspflicht und Zustimmung

Die betroffenen Personen müssen darüber informiert[5] werden, dass ihre personenbezogenen Daten erfasst werden und in welcher Form und zu welchem Zweck ihre Daten bearbeitet werden. Diese Information kann beispielsweise in Form einer Geheimhaltungserklärung erfolgen, die den betroffenen Personen übermittelt oder signalisiert wird. Die Informationspflicht bei einer automatisierten Einzelentscheidung ist gesondert geregelt[6].

In den folgenden drei Fällen ist eine ausdrückliche Zustimmung seitens der betroffenen Person erforderlich[7]:

- Bei der Bearbeitung sensibler Daten: Zu den so genannten „sensiblen“ Daten gehören Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, genetische Daten, biometrische Daten, Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen sowie Daten über Massnahmen der sozialen Hilfe.
- Bei einem Profiling mit hohem Risiko durch eine Privatperson: Heutzutage kann anhand von Bewegungsdaten festgestellt werden, wer wen wann und wo trifft. Diese Informationen gelten als besonders schützenswert. Die Bearbeitung von Daten, die die Erstellung eines genauen Persönlichkeitsprofils durch Zusammenführen von Daten aus unterschiedlichen Quellen ermöglichen, ist streng geregelt und setzt insbesondere die ausdrückliche Zustimmung der betroffenen Person voraus.
- Bei einem Profiling durch ein Bundesorgan.

Ausnahmen von der Informationspflicht[8]:

- Die betroffene Person verfügt bereits über die entsprechenden Informationen;
- Die Bearbeitung ist gesetzlich vorgesehen;
- Es handelt sich beim Verantwortlichen um eine private Person, die gesetzlich zur Geheimhaltung verpflichtet ist;
- Die Daten werden zur Veröffentlichung in einem Medium nach Artikel 27 nDSG bearbeitet.

[3] Artikel 5 Buchstabe d nDSG
[4] Artikel 9 nDSG
[5] Artikel 19 nDSG
[6] Artikel 21 nDSG
[7] Artikel 6 Abs. 7 nDSG
[8] Artikel 20 nDSG

Werden die Daten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, wenn die Information nicht möglich ist oder einen unverhältnismässigen Aufwand erfordert.

Schliesslich kann der Verantwortliche die Mitteilung der Informationen einschränken, aufschieben oder darauf verzichten, wenn überwiegende Interessen Dritter die Massnahme erfordern oder wenn die Information den Zweck der Bearbeitung vereitelt[9].

1.3. Grundsatz der Sicherheit

Der Verantwortliche muss durch geeignete technische Massnahmen (z.B. Authentifizierung mit Passwort, Verschlüsselung, regelmässige Datensicherungen usw.) und organisatorische Massnahmen (z. B. Schulung, Anweisungen, Kontrollen usw.) dafür sorgen, dass die Bearbeitung der Daten sicher ist und Verletzungen der Datensicherheit vermieden werden.[10]

Pflicht zur Meldung von Verletzungen der Datensicherheit[11]: Verletzungen der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen, sind dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) so rasch als möglich zu melden[12]. Dies ist etwa der Fall, wenn die Verletzung körperliche, materielle oder immaterielle Schäden bei der Person verursachen kann, deren Daten Gegenstand der Verletzung waren.
Die Verletzung ist ausserdem der betroffenen Person mitzuteilen, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

1.4. Recht auf Zugang

Die betroffene Person verfügt künftig über ein Recht auf Zugang zu den sie betreffenden Daten. Das Gesetz benennt die Informationen, die der Person, die ihr Recht ausüben möchte, mitzuteilen sind, damit sie ihre Ansprüche geltend machen kann und die Transparenz gewährleistet ist[13].

1.5. Verpflichtung zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten

Die Verantwortlichen (und Auftragsbearbeiter) führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten[14]. Ausnahmen sind für natürliche Personen und für Unternehmen vorgesehen, die weniger als 250 Mitarbeitende beschäftigen und deren Datenbearbeitung sich nicht auf umfassende sensible Daten bezieht oder nur ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt[15].

[9] Artikel 20 Absatz 3 nDSG
[10] Artikel 8 nDSG
[11] Artikel 24 Absatz 4 nDSG
[12] Artikel 24 nDSG
[13] Artikel 25 nDSG
[14] Artikel 12 nDSG
[15] Artikel 24 neue Verordnung zum Bundesgesetz über den Datenschutz (nVDSG)

1.6. Verschärfte strafrechtliche Sanktionen[16]

Bussgelder können künftig bis zu CHF 250’000 CHF betragen (derzeit CHF 10’000). Die Bussgelder richten sich nicht gegen das Unternehmen, sondern gegen die verantwortliche natürliche Person (Mitglied des Verwaltungsrates und/oder der Direktion).

2. Fazit

Das neue Datenschutzgesetz geht mit zahlreichen Änderungen, neuen Pflichten und strengeren Anforderungen an den Schutz von Daten einher.

Die fundamentale Überarbeitung des Gesetzes erfordert eine intensive Selbstbeobachtung der Schweizer Unternehmen, für die noch einige Monate Zeit besteht. Dabei wird es einerseits darum gehen, das derzeitige Mass an Konformität mit den neuen Datenschutzanforderungen zu bestimmen, aber auch darum, geeignete Massnahmen und Prozesse zu implementieren, die es ihnen ermöglichen, einen optimalen und gesetzlich konformen Datenschutz zu garantieren.

Der Inhalt dieser Veröffentlichung stellt keine abschliessende juristische Einschätzung oder Beratung dar. Wenn Sie weitere Informationen zu diesem Thema wünschen, wenden Sie sich gerne per E-Mail an die Kanzlei Frôté & Partner unter info@frotepartner.ch.

[16] Artikel 60 ff. nDSG