FAQ zum revidierten Schweizer Datenschutzgesetz

Zwölf Fragen und Antworten

THOUVENIN

Wann ist das revidierte Datenschutzgesetz anwendbar?

THOUVENIN

Das revidierte Datenschutzgesetz gilt für private Personen, insbesondere Unternehmen, welche Personendaten von natürlichen Personen bearbeiten.

Das Bearbeiten erfasst nahezu jeden Umgang mit Personendaten, so beispielsweise das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben (d.h. das Übermitteln oder Zugänglichmachen), Archivieren, Löschen oder Vernichten von Daten. Erfasst ist jede Bearbeitung und zwar unabhängig davon, ob diese elektronisch, physisch oder in einer anderen Weise erfolgt.

THOUVENIN

Was sind Personendaten?

THOUVENIN

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

Zu denken ist etwa an Namen oder Kontaktdaten von Kunden oder Mitarbeitenden sowie andere Angaben, die indirekt ermöglichen, eine Person zu identifizieren. Dazu gehören Standortdaten, IP-Adressen, Mitarbeiternummern, etc.

THOUVENIN

Muss ich die betroffenen Personen über die Datenbearbeitung informieren?

THOUVENIN

Ja, das revidierte Datenschutzgesetz sieht eine Informationspflicht bei der Beschaffung von Personendaten vor. Neu müssen die betroffenen Personen (z.B. Kunden oder Mitarbeitende) mit folgenden Mindestinformationen versorgt werden:

- Identität und die Kontaktdaten des Verantwortlichen
- Bearbeitungszwecke
- Empfänger oder Kategorien der Empfänger, denen Personendaten bekannt gegeben werden
- Bei Datenbekanntgabe ins Ausland: Land und die Garantie, auf welche sich die Auslandbekanntgabe abstützt (z.B. die EU-Standardvertragsklauseln)

Die Informationen werden beispielsweise in Datenschutzerklärungen, Datenschutzhinweisen oder in Verträgen zur Verfügung gestellt. Wichtig ist, dass die Informationen leicht zugänglich, verständlich, transparent und präzise sind.

THOUVENIN

Braucht es immer ein Verzeichnis über die Bearbeitungstätigkeiten?

THOUVENIN

Nein, aber… grundsätzlich muss ein sog. Verzeichnis über die Bearbeitungstätigkeiten mit einem gewissen Mindestinhalt geführt werden. Allerdings hat der Bundesrat bestimmte Ausnahmen in der Verordnung vorgesehen. So müssen Unternehmen, die weniger als 250 Mitarbeitende beschäftigen grundsätzlich kein Verzeichnis führen, ausser sie bearbeiten besonders schützenswerte Daten (z.B. Gesundheitsdaten) oder führen Profiling mit hohem Risiko durch.

Zwar besteht eine Ausnahme für KMUs, jedoch ist es oft trotzdem sinnvoll, ein Verzeichnis über die Bearbeitungstätigkeiten zu führen. Einerseits werden dadurch sämtliche Datenbearbeitungen systematisch erfasst. Andererseits hilft die systematische Erfassung der Datenbearbeitung, um andere Pflichten zu erfüllen. So zeigt ein Verzeichnis beispielsweise auf, wo Datenschutzerklärungen fehlen oder wo Personendaten im Falle eines Auskunftsbegehrens auffindbar sind.

Muss in der Schweiz immer ein Datenschutzberater (das Schweizer Pendant zum EU-Datenschutzbeauftragten) ernennt werden?

THOUVENIN

Nein, private Unternehmen müssen keinen Datenschutzberater ernennen, können dies aber auf freiwilliger Basis tun.

Auch wenn keine Pflicht besteht, einen Datenschutzberater formell zu benennen, ist es in der Regel hilfreich und sinnvoll, wenn sich intern eine Person dem Thema annimmt und entsprechende Expertise aufbaut.

THOUVENIN

Wer ist ein Auftragsbearbeiter und was ist bei dessen Beizug zu beachten?

THOUVENIN

Auftragsbearbeiter sind Dritte, welche im Auftrag und auf Weisung eines anderen Unternehmens (dem Verantwortlichen) in irgendeiner Form Personendaten bearbeiten. Beispiele für Auftragsbearbeiter sind der IT-Support, Clouddienstleister, externe Lohnbuchhalter, Newsletter-Tool-Anbieter, Betreiber von Call-Center, externe Aktenvernichter oder ein Hosting-Provider.

Sobald ein Auftragsbearbeiter für die Bearbeitung von Personendaten hinzugezogen wird, sollte ein Vertrag abgeschlossen werden (sog. Auftragsbearbeitungsvertrag), der sicherstellt, dass Personendaten nur so bearbeitet werden, wie der Verantwortliche es tun darf, der Auftragsbearbeitung keine Geheimhaltungspflichten entgegenstehen, der Auftragsbearbeiter die Datensicherheit gewährleistet und Unterauftragnehmer durch den Verantwortlichen genehmigt werden.

Haben Auftragsbearbeiter ihren Sitz im Ausland, muss der Verantwortliche sicherstellen, dass im Staat, in welchen Personendaten übermittelt werden, ein angemessenes Datenschutzniveau besteht. Ist der betroffene Staat im Anhang der Datenschutzverordnung aufgeführt, kann davon ausgegangen werden, dass ein angemessenes Datenschutzniveau besteht. Fehlt der Staat auf der Liste in der Datenschutzverordnung, muss mittels anderer Garantien sichergestellt werden, dass ein angemessenes Datenschutzniveau besteht. In der Praxis sehr relevant sind die sog. EU-Standardvertragsklauseln. Zudem muss jeweils ein sog. Transfer Impact Assessment durchgeführt werden. Darin werden die Risiken der Datenübermittlung systematisch erfasst, bewertet und Massnahmen zur Risikominimierung definiert.

THOUVENIN

Was sind Datenschutz-Folgen-abschätzungen und wann müssen sie durchgeführt werden?

THOUVENIN

Datenschutz-Folgenabschätzungen ("DSFA") sind strukturierte Risikobeurteilungen. Darin werden die Risiken, die für die betroffenen Personen bestehen, systematisch erfasst und festgehalten, wie mit den erfassten Risiken umgegangen werden soll (z.B. wie diese minimiert werden können). Die Risikobeurteilung erfolgt vor der Bearbeitung der Daten und ist dann zwingend, wenn die zukünftige Bearbeitungstätigkeit voraussichtlich ein hohes Risiko für die betroffenen Personen mit sich bringt (z.B. bei umfangreichen Bearbeitungen von besonders schützenswerten Daten oder der systematischen und umfangreichen Überwachung von öffentlichen Bereichen).

Insofern sollte für neue Datenbearbeitungen jeweils eine Vorprüfung der mit der Datenbearbeitung verbundenen Risiken stattfinden, sodass ggf. ein DSFA durchgeführt werden kann, soweit notwendig. Es lohnt sich somit, einen internen Prozess festzulegen. Schliesslich muss der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte konsultiert werden, sofern nach der DSFA nach wie vor hohe Risiken für die betroffenen Personen bestehen.

THOUVENIN

Was ist eine Verletzung der Datensicherheit und in welchem Zeitraum muss diese gemeldet werden?

THOUVENIN

Eine Verletzung der Datensicherheit liegt dann vor, wenn Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden. Werden Personendaten Unbefugten offengelegt oder zugänglich gemacht, liegt ebenfalls eine Verletzung der Datensicherheit vor. Beispiele für solche Verletzungen sind Ransom-Attacken und andere Hackerangriffe sowie die unerlaubte Weitergabe von Personendaten, ein E-Mail-Fehlversand, Datendiebstahl, etc.

Sofern eine Verletzung der Datensicherheit festgestellt wird, muss bestimmt werden, welche Risiken für die betroffenen Personen bestehen (z.B. Datenmissbrauch, Identitätsdiebstahl, etc.). Führt die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die betroffenen Personen, muss die Verletzung so rasch wie möglich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gemeldet werden. Das revidierte Datenschutzgesetz lässt im Vergleich zu ihrem europäischen Pendant etwas mehr Spielraum bezüglich der Meldefrist. Ob sich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte an der in der EU geltenden 72 Stunden-Frist orientieren wird, wird sich zeigen müssen.

Schliesslich müssen die betroffenen Personen über die Verletzung der Datensicherheit informiert werden, wenn es zu ihrem Schutz erforderlich ist, d.h. insbesondere, wenn sie selbst schadensminimierende Massnahmen treffen können (z.B. durch Sperrung von Kreditkarten oder Änderung von Passwörtern) oder der Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragte dies verlangt.

THOUVENIN

Welche Informationen müssen einer betroffenen Person bei einem Auskunftsgesuch zur Verfügung gestellt werden und wie schnell muss die Auskunft erfolgen?

THOUVENIN

Auf ein Auskunftsgesuch hin müssen der betroffenen Person nach deren Identifikation folgende Informationen mitgeteilt werden:

- Identität und die Kontaktdaten des Verantwortlichen
- Bearbeitete Personendaten
- Bearbeitungszwecke
- Aufbewahrungsdauer oder die Kriterien der Festlegung dieser Dauer
- Verfügbare Angaben über die Herkunft der Personendaten, sofern diese nicht von der betroffenen Person erhoben wurden
- Ggf. das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht
- Ggf. Empfänger oder Kategorien der Empfänger, denen Personendaten bekannt gegeben werden sowie das Land und die Garantie, auf welche sich die Auslandbekanntgabe abstützt (z.B. die EU-Standardvertragsklauseln)

Ein Gesuch einer betroffenen Person muss in der Regel innert 30 Tagen kostenlos beantwortet werden.

THOUVENIN

Bis wann muss das revidierte Datenschutzgesetz umgesetzt sein?

THOUVENIN

Da keine Übergangsfristen vorgesehen sind, müssen die neuen Pflichten des revidierten Datenschutzgesetzes bis zum 1. September 2023 umgesetzt werden. Dann tritt das Gesetz in Kraft.

THOUVENIN

Welche Sanktionen drohen, wenn das revidierte Datenschutzgesetz nicht umgesetzt wird?

THOUVENIN

Für ausgewählte vorsätzliche Handlungen und Unterlassungen werden Bussen für private Personen bis zu CHF 250’000 angedroht. Auf Antrag bestraft wird die Missachtung von Informations-, Auskunfts- und Mitwirkungspflichten sowie die Verletzung von Sorgfaltspflichten (z.B. Auftragsbearbeitung, Datenbekanntgabe ins Ausland oder Mindestanforderungen an die Datensicherheit) und der beruflichen Schweigepflicht. Hingegen werden die Missachtung von Verfügungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten von Amtes wegen verfolgt. Die Busse zielt auf die verantwortliche natürliche Person im Unternehmen ab (z.B. Leitungspersonen).

Neu kann aber auch das Unternehmen selbst mit bis zu CHF 50’000 gebüsst werden, wenn die Ermittlung der strafbaren natürlichen Person innerhalb des Unternehmens einen unverhältnismässigen Untersuchungsaufwand mit sich ziehen würde.

THOUVENIN

Wie kann ein Unternehmen vorgehen, um das revidierte Datenschutzgesetz umzusetzen?

THOUVENIN

Grundsätzlich gibt es keinen "one size fits all"-Ansatz, weil die meisten Unternehmen einen sehr unterschiedlichen Stand bezüglich bestehender Compliance-Massnahmen aufweisen. In der Praxis hat sich aber ein strukturiertes Vorgehen bewährt:

1. Sensibilisierung und Projektplanung
2. Ermittlung des Status Quo und Durchführung einer Gap-Analyse
3. Priorisieren und Umsetzen der Massnahmen aus der Gap-Analyse
4. Monitoring der Entwicklungen und ggf. Anpassung bestehender Dokumente und Prozesse

THOUVENIN

Weitere Fragen?

Marco S. Meier

Counsel | Rechtsanwalt

MLaw | CIPP/E | Informatiker EFZ

m.meier@thouvenin.com

www.thouvenin.com

THOUVENIN