PROBSTPARTNER

Neues Datenschutzrecht – Schweiz und EU

Die 2018 in Kraft tretenden Änderungen des Datenschutzrechts haben weitreichende Konsequenzen für Schweizer Unternehmen und Organisationen. Die heute verwendeten Vertragsklauseln und Datenschutzerklärungen genügen den neuen Anforderungen nicht mehr. Verträge mit Auftragsbearbeitern, wie z.B. IT-Dienstleistern oder Cloud-Betreibern, müssen umfassende Datenschutzregeln enthalten. Die internen Abläufe zur Bearbeitung von Personendaten müssen überholt oder erst aufgesetzt und dokumentiert werden. Jetzt ist der Zeitpunkt, um die notwendigen Umsetzungsarbeiten an die Hand zu nehmen. Andernfalls drohen schmerzhafte Konsequenzen in Form von administrativen Massnahmen, hohen Bussen und Kundenverlusten.

Das Datenschutzrecht in der EU und der Schweiz erfährt derzeit fundamentale Änderungen. Das neue Recht in der EU gilt bereits ab Ende Mai 2018, während das Schweizer Datenschutzrecht voraussichtlich kurz darauf in Kraft tritt. Die Neuerungen zielen darauf ab, dem Datenschutz einen höheren Stellenwert in der Gesellschaft zu vermitteln, indem ein bewussterer Umgang mit eigenen und fremden Personendaten gefördert wird.

Strengere Gesetze

Um diesen Wandel herbeizuführen, werden die Rechte der Betroffenen ausgebaut und umfangreichere Informationspflichten sowie strengere Dokumentationsvorschriften eingeführt. Nach dem Willen des Gesetzgebers muss jedes Unternehmen genau beantworten können:

> **Wo erhebe ich welche Personendaten; wer hat für welche Zwecke Zugriff und wie lange speichere ich sie, bevor ich sie schliesslich vernichte oder anonymisiere.**

Verstösse gegen das Datenschutzrecht werden neu mit drastischen Sanktionen geahndet, neben hohen Bussen können bestimmte Verstösse auch zu persönlicher Haftung der Involvierten führen. Die Aufsichtsbehörden werden entsprechend ihren erweiterten Befugnissen ausgebaut.

Jetzt handeln

Damit ist absehbar, dass Unternehmen in Zukunft viel stärker in die Pflicht genommen und auch zur Verantwortung gezogen werden. Die Revision des Schweizer Datenschutzgesetzes ist zwar noch nicht abgeschlossen. Schweizer Unternehmen und Tochtergesellschaften von ausländischen Unternehmen sollten diese aber nicht abwarten, zumal die meisten ohnehin direkt vom EU Recht erfasst sind, welches ab 25. Mai 2018 einzuhalten ist. Zudem wird der Druck seitens der Geschäftspartner mit Sitz in der EU zunehmen, da sie die Einhaltung der neuen Vorgaben von ihren Lieferanten und Partnern verlangen müssen. Um konkurrenzfähig zu bleiben und diese Kunden nicht zu verlieren, sollten betroffene Unternehmen daher jetzt die Auswirkungen auf ihren Betrieb analysieren und die neuen Datenschutzregeln konsequent und adäquat umsetzen.

Wer ist betroffen?

Das neue Recht hat Auswirkungen auf praktisch alle Unternehmen und Organisationen. Auch Ihr Unternehmen ist betroffen, wenn Sie mindestens eine dieser Fragen mit Ja beantworten:

- Führen Sie eine Datenbank mit Personendaten, z.B. von Kunden oder Mitarbeitern?
- Haben Sie eine Webseite mit Web-Shop, Kontaktformular oder Cookies?
- Haben Sie Betrieb von IT-Systemen mit Personendaten an Dritte ausgelagert oder Personendaten in der Cloud gespeichert?
- Erbringen Sie IT-Dienstleistungen an Kunden in der Schweiz oder in der EU?

Was sind die Neuerungen?

Die Neuerungen sind vielseitig. Eine kleine Auswahl der wichtigsten Punkte:

- *Umfassendere Informationspflichten:* Das neue Recht verlangt höhere Transparenz für die Betroffenen. So muss in Zukunft viel umfassender informiert werden, wobei das Gesetz den Mindestinhalt vorgibt. Die heute üblichen Datenschutzerklärungen ("Privacy Policy") genügen in den meisten Fällen den neuen Anforderungen nicht. So muss u.a. über die Dauer der Datenspeicherung und über Profilingaktivitäten inklusive deren Logik und Folgen informiert werden.
- *Strengere Voraussetzungen für Auslagerungen*: Die Sorgfalts- und Regelungspflichten bei externer Bearbeitung von Personendaten (z.B. durch einen IT-Dienstleister oder Cloud-Provider) werden erhöht – sowohl für die Auftraggeber (Kunden) wie auch für die Leistungserbringer (Auftragnehmer). Vor allem im Anwendungsbereich der EU Gesetzgebung ist die Auftragsdatenbearbeitung künftig viel detaillierter in einem Vertrag zu regeln.
- *Ausbau der Rechte der Betroffenen:* Die Rechte der Betroffenen werden deutlich ausgebaut. Den betroffenen Personen müssen in vielen Bereichen echte Wahlmöglichkeiten eingeräumt werden. Neu haben Betroffene zudem das Recht, die Nutzung ihrer Personendaten teilweise einzuschränken. Soweit das EU-Recht Anwendung findet, können sie zudem die Übertragung ihrer Personendaten auf einen Dritten oder deren Rückgabe verlangen (Datenübertragbarkeit, "Data Portability").

- *Meldung von Datenschutzverstössen:* Neu müssen Verletzungen der Datensicherheit ("Data Breaches"), die Personendaten betreffen, unverzüglich der Aufsichtsbehörde gemeldet werden, was entsprechende interne Abläufe bedingt ("Incident Management"). Unter Umständen sind auch die Betroffenen zu benachrichtigen.
- *Datenschutz-Folgenabschätzung*: Bei Datenbearbeitungsvorgängen mit einen hohen Risiko für die betroffenen Personen, z.B. bei einem Profiling oder umfangreicher Bearbeitung besonders schützenswerter Personendaten, muss eine Datenschutz-Folgenabschätzung vorgenommen und unter Umständen die Aufsichtsbehörde konsultiert werden.

Zu diesen ausgewählten Punkten tritt eine Dokumentationspflicht hinzu. Die Unternehmen müssen ihre Prozesse und Systeme anpassen oder neu aufsetzen, um die Anforderungen einhalten zu können.

Warum müssen Sie sich für Datenschutz-Compliance interessieren?

Compliance, also die Einhaltung der rechtlichen Vorgaben und damit auch des Datenschutzrechts ist eine der Hauptaufgaben des Verwaltungsrates und der Unternehmensleitung. Verstösse gegen Datenschutzregeln können neben Reputationsschaden Bussen von bis zu EUR 20 Mio. oder 4% des weltweiten Jahresumsatzes zur Folge haben. Die Mitglieder von Verwaltungsrat und Geschäftsführung haften zudem persönlich für Schaden, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen, zum Beispiel weil sie Risiken nicht erkennen oder nicht dafür sorgen, dass innerhalb des Unternehmens die gesetzlichen Regelungen eingehalten werden.

Neben der Vermeidung von Sanktionen und Haftungsrisiken bringt die Umsetzung der datenschutzrechtlichen Anforderungen den Unternehmen einen betrieblichen Nutzen. Das Datenschutzrecht zwingt Organisationen zu einem strukturierten, kontrollierten und vorausschauenden Umgang mit Personendaten. Dies ermöglicht gleichzeitig, das Potential der Daten für das Unternehmen besser zu nutzen, etwa im Bereich von datenbasierten oder digitalisierten Geschäftsmodellen ("Big Data") und für gezieltere Kundenansprache. Zudem können allfällige bestehende Doppelspurigkeiten oder nicht mehr benötigte Applikationen entdeckt und beseitigt werden.

Drei Schritte zur Datenschutz-Compliance

Das Datenschutzrecht verfolgt in vielen Bereichen einen risikobasierten Ansatz. Es sind jene Massnahmen zu treffen, die angemessen sind angesichts des potentiellen Risikos für die Persönlichkeitsrechte der betroffenen Person. Um die erforderlichen Massnahmen definieren zu können, müssen zuerst die eigenen Datenbearbeitungen verstanden werden. Wir empfehlen eine Umsetzung in drei Schritten:

	Inhalt	Ziel	Unsere Dienstleistungen
1	**IST Aufnahme des Ist-Zustandes**	Das Unternehmen hat einen Überblick über die bearbeiteten Personendaten und die damit verbundenen Risiken: Wer bearbeitet wie welche Personendaten wozu auf welcher Grundlage und wie lange; Wie werden Betroffenenrechte erfüllt; Auf welcher Basis erfolgen Übermittlungen ins Ausland und wohin; Welche Verträge bestehen mit Auftragsdatenbearbeitern; Welche Risiken bestehen.	Bereitstellung Fragebogen und Ablauf; Unterstützung bei oder Durchführung der Sachverhaltsaufnahme; Erste Grobanalyse mit Empfehlung für Priorisierung der zu prüfenden Bearbeitungen (Ampel-System).
2	**SOLL/GAP Compliance-Prüfung und Gap-Analyse**	Das Unternehmen hat die Massnahmen und die Umsetzungsplanung festgelegt, um die datenschutzrechtlichen Anforderungen zu erfüllen.	Prüfung der Bearbeitungen auf Datenschutzkonformität; Identifikation der notwendigen Massnahmen für Compliance; Empfehlungen für Vorgehen und Priorisierung der Massnahmen.
3	**UMSETZEN Umsetzung der Massnahmen**	Das Unternehmen hat die nötigen Massnahmen zur Einhaltung des Datenschutzes umgesetzt und kann die Umsetzung der datenschutzrechtlichen Vorgaben gegenüber möglichen Ansprechern (Betroffene, Aufsichtsbehörden, Gerichte, Geschäftspartner) belegen.	Erstellen der notwendigen Dokumente, Reglemente, Verträge etc.; Unterstützung bei der Implementierung von Prozessen und Massnahmen.

Unsere Expertise

Datenschutz- und Technologierecht ist ein Schwerpunkt unserer Kanzlei. Julia Bhend wird von unabhängigen Rankings wie Chambers and Partners, Best Lawyers und Who's Who Legal als eine der führenden Datenschutz- und IT-Anwälte in der Schweiz genannt. Kaj Seidl-Nussbaumer berät ebenfalls seit Jahren im Datenschutzrecht. Wir haben Klienten in verschiedenen Branchen entsprechend unterstützt. Eine Auswahl:

- International tätiges IT-Unternehmen: Beratung betreffend Einhaltung des Datenschutzrechts und der Informationssicherheit bei der Bearbeitung von Personendaten von Kunden in der Finanzindustrie und öffentlichen Verwaltung
- Internationales Pharmaunternehmen: Laufende Beratung in Bezug auf die Einhaltung des Datenschutzrechts in der Schweiz, insb. auch im Zusammenhang mit gruppeninternen Datenübermittlungen und zentralisierten IT-Systemen
- Internationaler Hersteller von Technologiegütern: Laufende Beratung in Bezug auf die Einhaltung des Datenschutzrechts in der Schweiz, insb. auch im Zusammenhang mit gruppeninternen Datenübermittlungen und zentralisierten IT-Systemen
- Internationales Industrieunternehmen: Unterstützung in Industry 4.0 / Digitalisierungsinitiative, inkl. Analyse der zu treffenden Massnahmen für Datenschutz-Compliance (EU und Schweiz)
- Ausländischer Automobilhersteller: Beratung in Bezug auf die Implementierung eines CRM Systems, das Sammeln und Nutzen von Daten der Kunden für Überwachung und Wartung der Fahrzeuge in der Schweiz
- Internationales Unternehmen im Anlagebau und in der Gebäudetechnik: Laufende Beratung betreffend Einhaltung des Datenschutzrechts in der Schweiz, u.a. im Zusammenhang mit gruppeninternen Übermittlungen und zentralisierten IT-Systemen
- Schweizer Hersteller von Geräten und Apps im Gesundheitsbereich: Beratung betreffend Umsetzung der datenschutzrechtlichen Anforderungen beim Einsatz von Medizinprodukten und Smartphone-Apps bei Patienten/Spitälern in der Schweiz.

Kontakt

Julia Bhend, Partner, julia.bhend@probstpartner.ch

Kaj Seidl-Nussbaumer, Associate, kaj.seidl-nussbaumer@probstpartner.ch