NEWSLETTER APRIL 2018

Agenda 2018/2019: Datenschutz.

Are you ready for the (near) future in data protection?

Pflichten und Anforderungen aus der Europäischen Datenschutzgrundverordnung (EU DSGVO) und dem revidierten Datenschutzgesetz (DSG)

- Implementierung der neuen und umfassenden Compliance-Funktion «Datenschutzberaterin/-berater» («Data Protection Officer») nach Art. 9 E-DSG (nach Art. 37 ff. DSGVO: Datenschutzbeauftragter) in Abhängigkeit der Grösse des Unternehmens und der Intensität der Datenbearbeitung
- Erstellen eines Verzeichnisses der Bearbeitungstätigkeiten (Datenschutzverzeichnis) nach Art. 11 E-DSG und Festlegen der Prozesse zur periodischen Überarbeitung (rollend)
- Bilden eines Prozesses für die Datenschutz-Folgenabschätzung gemäss Art. 20 E-DSG

Einleitung – Umfassender Schutz für Personendaten und strenge Anforderungen an die Verantwortlichen

Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Durch die rege Teilnahme an Social Media Plattformen und die zunehmende Inanspruchnahme von Online-Diensten machen auch natürliche Personen ihre persönlichen und darüber hinaus besonders schützenswerte Daten öffentlich und weltweit zugänglich. Die technische Entwicklung und Veränderungen des wirtschaftlichen und gesellschaftlichen Lebens rechtfertigen daher ein hohes Datenschutzniveau.[1]

Aktuelle Skandale von Datenverkauf an Dritte ohne Information und Zustimmung der Dateninhaber verdeutlichen das enorme Reputationsrisiko bei unausreichenden datenschutzrechtlichen Massnahmen und internen Kontrollen bei den verantwortlichen Unternehmen.

Stichworte wie automatisierte Verarbeitung bzw. Bearbeitung[2] personenbezogener Daten für wirtschaftliche und andere Zwecke («Profiling»[3]), fehlende Transparenz und ungenügende Zustimmung über den Bearbeitungszweck ausserhalb des operativen Betriebs (z.B. Marketing), Zukauf von Daten oder Datenübermittlung an Dritte (Auftragsbearbeitung) oder ins Ausland (EU) zeigen einige der Problemfelder in Bezug auf die Rechte der Betroffenen auf, die der Gesetzgeber durch die Totalrevision des Datenschutzgesetzes (DSG) beheben will.

Das revidierte DSG mit umfassenden neuen Pflichten und Anforderungen tritt am **1. Januar 2019** in Kraft. Bereits ab **25. Mai 2018** gilt die **EU-Datenschutz-Grundverordnung** (DSGVO). Inhaltlich bestehen nur wenige Unterschiede zwischen den beiden Erlassen.

Wer ist betroffen?

Das **DSG** gilt für private Personen (hier: verantwortliche Unternehmen) und Bundesorgane, die Personendaten natürlicher Personen bearbeiten.

Die **DSGVO** (General Data Protection Regulation/GDPR) ist für alle Unternehmen im EU- und EWR-Raum bindend und gilt ebenfalls für Unternehmen ausserhalb des EU- und EWR-Raums, welche Dienstleistungen und Produkte für EU- und EWR-Bürger anbieten und Daten von EU- und EWR-Bürgern verarbeiten. Die Verordnung ist auch dann anwendbar, wenn die Daten dazu dienen, das Verhalten der Personen zu beobachten, z.B. die Analyse der Daten von Website Besuchern oder von App-Nutzern aus der EU. Das EU-Recht wirkt sich somit auch auf Schweizer Exporteure, Versandhändler, Betreiber von Plattformen für Online-Bestellungen sowie für (Finanz-)Dienstleister aus, die ihre Leistungen Kunden in der EU anbieten. Diese Unternehmen müssen einen Vertreter in der EU benennen, es sei denn, sie bearbeiten Daten von in der EU ansässigen Personen nur gelegentlich[4].

---

1 Vgl. Erw. 6 DSGVO.

2 Der Begriff «Bearbeiten» ist gemäss Art. 4 lit. d E-DSG weit gefasst. Unter «Bearbeiten» fällt «jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten»; ebenso der Begriff in Art. 4 Ziffer 2 DSGVO.

3 Art. 4 lit. f E-DSG: zu verstehen als «Bewertung bestimmter Merkmale einer Person auf der Grundlage von *automatisiert bearbeiteten Personendaten*, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen» (ebenso der Begriff in Art. 4 Ziff. 4 DSGVO).

4 Vgl. Art. 27 DSGVO.

Schutzzweck der DSGVO (Allgemein)

Die EU Datenschutz-Grundverordnung ersetzt die bislang geltende und aus dem Jahr 1995 stammende Richtlinie 95/46/EG (Datenschutzrichtlinie) und die auf deren Grundlage erlassenen nationalen Datenschutzgesetze.

Mit der DSGVO wird der Datenschutz in der Europäischen Union erstmals auf eine einheitliche rechtliche Grundlage gestellt. Inhaltlich führt die DSGVO zu verschiedenen wesentlichen Neuerungen, wie dem «Recht auf Vergessen», wonach betroffene Personen ihre Daten im Web durch die Datenverarbeiter löschen lassen können, oder der „One-Stop-Shop-Ansatz", gemäss welchem Datenschutzverletzungen von den Betroffenen direkt bei der Datenschutzbehörde in ihrem Mitgliedstaat geltend gemacht werden können, unabhängig davon, wo die Verletzung stattgefunden hat.

Harte und einschneidende Sanktionen

Unternehmen, die gegen die neuen Datenschutzregeln verstossen, können mit einer Geldbusse von bis zu 10 Mio. Euro oder im Fall eines Unternehmens von bis zu 2 % ihres gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs bestraft werden, je nachdem, welcher der Beträge höher ist.[5]

Maximale Geldstrafen von bis 20 Mio. Euro bzw. 4 Prozent des Jahresumsatzes können verhängt werden, sofern Verstösse der Verantwortlichen vorliegen, insbesondere gegen

a) die Grundsätze für die Verarbeitung, einschliesslich der Bedingungen für die Einwilligung;
b) die Rechte der betroffenen Person;
c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation.[6]

Kleineren Unternehmen drohen keine derartigen Sanktionen, wenn es sich um erstmalige, versehentliche oder kleinere Verstösse handelt.

Verschärfte Regelungen

Daneben sieht die DSGVO zum Teil verschärfte Regelungen zu zentralen Punkten des Datenschutzrechts vor, wie im Zusammenhang mit

- der Information der Betroffenen über die Verarbeitung ihrer Daten,
- der Notwendigkeit zur Einholung der Zustimmung der Betroffenen,
- dem Inhalt der vertraglichen Regelung bei der Verarbeitung von Daten durch Dritte (Auftragsdatenverarbeitung)

- die Voraussetzungen zur Übermittlung von Personendaten in EU-Drittländer.

Die Totalrevision des DSG berücksichtigt im Wesentlichen die Anforderungen und Inhalte der EU.

Pflichten und Anforderungen für Unternehmer

Jeder, der nur in irgendeiner Art und Weise im Unternehmen Daten mit Personenbezug (Name, Adresse, Telefonnummer, E-Mail Adresse) speichert, bearbeitet oder weiterleitet, fällt unter das DSG bzw. die DSGVO.

Die Verarbeitung von personenbezogenen Daten muss immer einem definierten Zweck zugeordnet werden. Eine Weiterverwendung für andere Zwecke darf nicht ohne Einverständnis der betroffenen Person erfolgen (Zweckbindung).

Unternehmen müssen im Weiteren gewährleisten, dass personenbezogene Daten korrekt sind. Falsche Daten müssen aktualisiert oder gelöscht werden (Richtigkeit). Die Speicherung von personenbezogenen Daten muss auf die Zeitdauer des Verwendungszwecks begrenzt sein (Speicherbegrenzung).

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen («privacy by design» & «privacy by default»)

Aufgrund der zunehmend technisch getriebenen Datenbearbeitungen sind gemäss Art. 6 E-DSG die verantwortlichen Unternehmen verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden. Diese Anforderungen sind ab der Planung zu berücksichtigen (nach dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Personen mit sich bringen). Dabei müssen die Voreinstellungen sicherstellen, «dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt».[7]

5 Vgl. Art. 83 Abs. 4 DSGVO.
6 Vgl. Art. 83 Abs. 5 DSGVO.
7 Analoge Anforderungen finden sich in Art. 25 DSGVO.

Wichtige datenschutzrechtliche Massnahmen zur fristgerechten Umsetzung dieser Pflichten – eine Auswahl

- Sicherstellen der Datenschutz-Grundsätze (rechtmässige Bearbeitung, Zweckvereinbarung, Richtigkeit der Daten und Datensicherheit[8]): Überarbeiten der Website/Homepage mit transparenten und für Dritte verständlichen datenschutzrechtlichen Hinweisen («Sicherheit und Datenschutz»), insbesondere:
  i) welche Daten von Kunden/Dritten werden gespeichert (Unterschied zwischen gesetzlich/geschäftlich notwendigen Daten und übrigen personenbezogenen Daten für wirtschaftlichen Nutzen);
  ii) wo (Website) bzw. auf welchen Formularen finden sich Einwilligungserklärungen und wie lange sollen diese gelten;
  iii) wie erfolgt die Bearbeitung der personenbezogenen Daten (Grundauftrag und zusätzliches Anbieten von Produkten und Services sowie Zwecke der Werbung und der Markt- und Meinungsforschung);
  iv) Hinweis auf die Möglichkeit des jederzeitigen Widerrufs von erteilten Zustimmungen (schriftlich oder telefonisch);
  v) Mitteilung, an wen - soweit gesetzlich zulässig oder vertraglich vereinbart - personenbezogene Informationen übermittelt werden (z.B. an Konzerngesellschaften innerhalb der Unternehmensgruppe; an beauftragte übrige Dienstleistungsunternehmen oder an Auskunfteien);
  vi) Mitteilung über die ergriffenen technischen und organisatorischen Sicherheitsmassnahmen zum Schutz der personenbezogenen Informationen.
- Prüfen und evtl. Etablieren der neuen und umfassenden Funktion des betrieblichen Datenschutzberaters (Ausarbeiten von Optionen) und Festlegen einer Datenschutzorganisation und von Verantwortlichkeiten innerhalb des Organisationsmodells (Matrix)
- Anlegen eines nach DSG notwendigen Verzeichnisses von Bearbeitungstätigkeiten (mit Inhalt Bearbeitungszweck; Beschreibung der Kategorien betroffener Personen und bearbeiteter Personendaten sowie Kategorien der Empfänger)
- Durchführen von Datenschutz-Folgenabschätzungen (bei Bearbeitung von besonders schützenswerten Personendaten oder bei Profiling)
- Sicherstellen der Informationspflichten für genügende Transparenz bei der Beschaffung von Personendaten (datenschutzrechtliche Hinweise)
- Grundlagen für die Anforderungen an die Einwilligung bzw. ausdrückliche Einwilligung
- Gewährleistung der Sicherheit von Personendaten, inkl. Kunden und Mitarbeiter (geeignete technische und organisatorische Massnahmen)
- Festgelegter Prozess mit zugeteilten Verantwortungsträgern in Fällen von Datenschutzverletzungen («data breaches»), inkl. Bewertung des Umfangs und der Folgen der Verletzung mit Massnahmen und des Prozesses für die Erstattung der unverzüglichen Meldung an den EDÖB
- Festgelegte Prozesse und technische Voraussetzungen zur Abgabe von vollständigen Auskünften an die Betroffenen, zur Datenberichtigung und zur Löschung

[8] Vgl. Art. 4 lit. g E-DSG; Art. 5 E-DSG; Art. 7 E-DSG (Anforderung mit geeigneten technischen und organisatorischen Massnahmen eine Verletzung der Datensicherheit vermeiden; insbesondere Überprüfung der IT-Security und der physischen Aufbewahrung von Dokumenten, inkl. Personalakten sowie den Berechtigungen für Mitarbeiter oder für Dritte und den Zutrittskontrollen).

Was ist zu tun? - Wie wird Ihr Unternehmen fit für diese datenschutzrechtlichen Anforderungen?

Aufgrund unserer Erfahrungen aus bisherigen Projekten unterstützen wir Ihr Unternehmen gerne bei der Umsetzung dieser datenschutzrechtlichen Anforderungen und empfehlen dabei folgende Schritte:

- Bestimmung von internen Verantwortlichen
- Durchführung einer Gap-Analyse (Assessment) als Vergleich zwischen Ist und Soll (Bildung von notwendigen Arbeitspaketen mit klaren Zuteilungen und Fristen zur Umsetzung)
- Analyse der Datenbestände, Prozesse und IT (Grundlage für Datenschutzverzeichnis)
- Umsetzung von Massnahmen wie Erstellung eines Datenschutzverzeichnisses, Prüfen der Verträge mit Auftragsbearbeitern, Gewährleistung der Datensicherheit
- Festlegen von Prozessen für die Gewährleistung des Datenschutzes für die Zukunft (internes Kontrollsystem/IKS und Compliance Control Programm/CCP).

Dr. Detlev Basse
Detlev Basse verfügt über langjährige Erfahrung in der Leitung von massgebenden Compliance-Projekten; aktuell Projektleiter Datenschutz für ein Finanzinstitut in der Ostschweiz.

Für Fragen in diesem Zusammenhang

Dieter C. Hauser
Founder, Managing Partner
dieter.hauser@icomply.ch

Detlev M. Basse
Senior Counsel & Compliance Specialist
detlev.basse@icomply.ch

icomply AG
Wiesenstrasse 7
CH-8008 Zürich

Phone +41 44 385 91 30

www.icomply.ch