WEKA Business Dossier

Datenschutz

Rechtliche Rahmenbedingungen und Umsetzung im Unternehmen

Business-Bereich

- Management
- Personal
- *IT & Recht*
- Erfolg & Karriere
- Kommunikation
- Marketing & Vertrieb
- Finanzen
- Führung

Sofort-Nutzen

Sie erfahren:

- Was die wichtigsten Bestimmungen des Datenschutzgesetzes sind
- Was die wichtigsten Prozesse sind, die zu implementieren sind
- Wie Sie ein Umsetzungsprojekt strukturieren

Sie erhalten:

- Praxiserprobte und pragmatische Umsetzungsvorschläge
- Diverse Checklisten
- Sicherheit im Umgang mit dem Datenschutzgesetz

Autorenteam

RA Dr. iur. Lukas Lezzi, CIPP/E, CIPM, CAS Forensics, ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Er hat in Zürich studiert und im Finanzmarktrecht dissertiert. Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.

Renisa Lajqi arbeitet als studentische Mitarbeiterin bei LezziLegal. Sie studiert Rechtswissenschaften in Zürich.

Mlaw Shqipe Beluhli arbeitet als Juristin bei LezziLegal. Sie hat in Zürich und Lausanne studiert. Sie betreut schwerpunktmässig datenschutzrechtliche und regulatorische Projekte.

Mlaw Luciana Viganò arbeitet als Juristin bei LezziLegal. Sie hat in Basel studiert. Bei LezziLegal berät sie Klienten im Datenschutz und Vertragsrecht.

Impressum

WEKA Business Dossier

Datenschutz

Projektleitung: Annika Küderli
Satz: Dimitri Gabriel
Korrektorat: Margit Bachfischer M.A. Bobingen, margit.bachfischer@web.de

WEKA Business Media AG
Hermetschloostrasse 77
8048 Zürich
Tel. 044 434 88 34
Fax 044 434 89 99

info@weka.ch
www.weka.ch
www.weka-library.ch

1. Auflage 2024

VLB – Titelaufnahme im Verzeichnis Lieferbarer Bücher:
ISBN: 978-3-297-02285-6

Inhaltsverzeichnis

1. Einführung

Mit dem Inkrafttreten des totalrevidierten Datenschutzgesetzes (DSG) am 1. September 2023 hat die Schweiz einen entscheidenden Schritt in Richtung zeitgemässer Datenschutzstandards unternommen. Der vorliegende Leitfaden beleuchtet nicht nur die rechtlichen Aspekte des neuen Datenschutzgesetzes, sondern hebt auch die Notwendigkeit hervor, den Datenschutz in die Unternehmens-Governance einzubeziehen.

Unternehmen müssen eine ganzheitliche Perspektive einnehmen und sämtliche relevanten Bereiche ihrer Governance-Struktur analysieren. In diesem Kontext erweist es sich als wichtig, die Wechselwirkungen zwischen dem DSG und anderen Unternehmensrichtlinien, Prozessen und Strukturen zu verstehen, weil das Thema Datenschutz in praktisch allen Aspekten eines Unternehmens zu berücksichtigen ist.

Das vorliegende Dossier hat zum Ziel, Unternehmen einen praxisnahen Leitfaden an die Hand zu geben, um die Anforderungen des neuen Datenschutzgesetzes in den verschiedenen Ebenen seiner Organisation möglichst pragmatisch umzusetzen. Es werden die wichtigsten Punkte zur Umsetzung aus Sicht der Autoren besprochen, aber das DSG wird nicht gesamthaft kommentiert.

Damit im Vornherein klar ist, was gemeint ist, sind hier ein paar Definitionen festgehalten:

a) **Verantwortlicher:** Eine natürliche Person, eine juristische Person oder ein Bundesorgan entscheidet über den Zweck und die Mittel der Datenbearbeitung.

b) **Personendaten:** Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden «betroffene Person») beziehen, z.B. Name, E-Mail-Adresse, Gehaltsdaten, Telefonnummer.

c) **besonders schützenswerte Personendaten:** Diese bilden eine Unterkategorie der Personendaten. Alle folgenden Daten erfordern einen besonderen Schutz und eine strengere Handhabung:
   - 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, die eine natürliche Person eindeutig identifizieren
   - Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen und
   - Daten über Massnahmen der sozialen Hilfe

d) **Bearbeitung:** Jeder Vorgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, z.B. Sammeln, Erfassen, Speichern, Verwenden, Ändern, Weitergeben, Löschen oder Vernichten von Personendaten.

e) **Auftragsbearbeiter:** Eine natürliche Person, eine juristische Person oder eine staatliche Einrichtung, die Personendaten im Auftrag und auf Weisung des für die Bearbeitung Verantwortlichen bearbeitet, z.B. ein Cloud-Dienstleister, der Personendaten für das Unternehmen hostet.

f) **Profiling:** Jede Form der automatisierten Bearbeitung von Personendaten zur Bewertung bestimmter persönlicher Aspekte, die sich auf eine natürliche Person beziehen, insbesondere zur Analyse oder Vorhersage von Aspekten.

g) **Profiling mit hohem Risiko:** Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

2. Konkreter Umsetzungsprozess im Unternehmen

Es ist in jedem Fall für die Umsetzung des DSG empfehlenswert, im Unternehmen eine kleine Projektorganisation vorzusehen. Umfang und Vorgehensweise für ein solches Unterfangen sind natürlich sehr individuell und hängen von verschiedenen Faktoren ab:

- Welche Bedeutung haben Datenbearbeitungen für das Unternehmen, insbesondere werden Datenbearbeitungen mit höheren Risiken durchgeführt, z.B. automatisierte Entscheidungen, Bearbeitung von besonders schützenswerten Personendaten etc.?
- Gibt es schon ein Datenschutz-Framework zur Europäischen Datenschutz-Grundverordnung (DSGVO), welches um die Anforderungen des DSG ergänzt werden könnte?
- Was sind die möglichen Ressourcen, die bereitgestellt werden können?

Grundsätzlich sollte aber in jedem Fall das Management eines Unternehmens als Stakeholder in einem solchen Projekt involviert sein, weil der Datenschutz letztlich alle Teile eines Unternehmens berührt. Als Unterstützung sollten in einem Projekt auch der interne Data Protection Officer (DPO) und Vertreter von Information Security mitwirken, sofern diese Funktionen vorhanden sind.

Bei kleinen Unternehmen ist es empfehlenswert, zumindest punktuell und insbesondere in der Konzeptphase des Projekts auf externe Unterstützung zurückzugreifen. Die Durchführung eines solchen Projekts kann aber dann sehr gut intern durchgeführt werden.

Generell empfiehlt es sich, ein solches Projekt nicht komplett extern durchführen zu lassen (z.B. durch Beauftragung einer Anwaltskanzlei oder eines Beratungsunternehmens), weil nach Abschluss des Projekts die neuen Prozesse auch tatsächlich intern akzeptiert und gelebt werden müssen. Dies kann nur erreicht werden, wenn die neuen Prozesse auch unternehmensintern erarbeitet werden.

Ein Umsetzungsprojekt könnte sich wie folgt gliedern:

- **Workstream 1 – Data Mapping:** In diesem Workstream werden die Datenflüsse und die Bearbeitungstätigkeiten analysiert. Weiter werden auch relevante Dienstleister und Verträge so identifiziert. Diese Arbeit ist die Voraussetzung für die weiteren Workstreams, kann aber auch für die initiale Erstellung eines Bearbeitungsverzeichnisses dienen.
- **Workstream 2 – Governance:** In diesem Workstream werden die internen Weisungen und Prozesse definiert und festgelegt. Der Umfang dieser internen Weisung ist von der Komplexität des Unternehmens und der Art der bearbeiteten Personendaten abhängig.
- **Workstream 3 – Verträge und Datenschutzerklärungen:** In diesem Workstream müssen die zuvor im Workstream 1 identifizierten Verträge und Datenschutzerklärungen angepasst bzw. neu erstellt werden. Hierbei stehen Auftragsbearbeitungsverträge und Datenschutzerklärungen für Kunden und Mitarbeitende im Fokus.
- **Workstream 4 – Information-Security:** Dieser Teil des Projekts deckt die Anforderungen an die Datensicherheit ab. Hier geht es darum, in einem ersten Schritt die konkreten Datensicherheitsmassnahmen zu definieren. Danach muss eine Gap-Analyse der in Workstream 1 identifizierten Systeme durchgeführt werden, um einen möglichen Handlungsbedarf festzustellen.

- **Workstream 5 – IT:** In diesem Workstream werden die identifizierten Systeme auf gewisse für den Datenschutz relevante Funktionen analysiert. Hier fällt insbesondere die Erfüllung der Auskunfts- und Löschungsrechte und der Datenportabilität in Betracht.
- **Workstream 6 – Implementierung:** In diesem abschliessenden Workstream werden insbesondere die neuen Prozesse implementiert, die Auftragsbearbeitungsverträge neu verhandelt, die Datenschutzerklärungen publiziert und die IT-Systeme angepasst. Die Anpassung von IT-Systemen hat in der Regel eine längere Vorlaufszeit, weshalb diese Implementierungsmassnahme zu priorisieren ist.

Workstream 1 und 2 können zuerst durchgeführt werden. Workstream 3–5 hängen von 1 und 2 ab und können erst begonnen werden, nachdem die für diese Workstreams relevanten Themen in Workstream 1 und 2 abgeschlossen wurden. Workstream 6 erfolgt dann nachgelagert zu den vorgehenden Workstreams.