AUSGABE 07
JULI/AUGUST 2025

binder rechtsanwälte

WEKA

# DATENSCHUTZ

FÜR SCHWEIZER UNTERNEHMEN UND INSTITUTIONEN

## Datenschutzrechtliche Haftung der Geschäftsleitung und des Verwaltungsrats

Mehr dazu auf Seite 2

## Risikominimierende Massnahmen – Datenschutzerklärung

Mehr dazu auf Seite 4

## Prozesse für den Umgang mit Auskunftsbegehren und Data Breaches

Mehr dazu auf Seite 7

## Beizug von Auftragsbearbeitern – Anleitung zur Risikoreduktion

Mehr dazu auf Seite 10

In dieser Ausgabe

# VR und GL – Risiken kennen und minimieren

**Compliance oder Konsequenz – Datenschutz beginnt im Kopf der Führung**

Datenschutz ist ein Thema, das spätestens seit dem Inkrafttreten des totalrevidierten Datenschutzgesetzes der Schweiz den Weg in die Köpfe der Allgemeinheit gefunden hat. Dies hat nicht nur die Risikobeurteilung in Bezug auf das Thema Datenschutz verändert, sondern ist auch in den Verwaltungsräten, Geschäftsleitungen oder anderen Entscheidgremien der Unternehmen angekommen.

In der Praxis hat sich gezeigt, dass Datenschutz sich dann ernsthaft in der DNA eines Unternehmens festsetzt, wenn das Thema von der Führungsebene – insbesondere vom Verwaltungsrat und von der Geschäftsleitung – als relevant identifiziert wurde und die entsprechenden internen Vorgaben glaubwürdig vorgelebt werden. In letzter Konsequenz bedeutet dies, dass sowohl Verwaltungsräte als auch Geschäftsleitungsmitglieder gewisse Grundzüge der datenschutzrechtlichen Anforderungen kennen und die Umsetzung dieser intern aktiv einfordern müssen. Zentral dabei sind nicht nur die Themen zur datenschutzrechtlichen Haftung der Führungsriege, sondern auch inhaltliche Aspekte, welche wesentlich zur Minimierung der datenschutzrechtlichen Risiken beitragen. Diese Ausgabe soll zu diesem Grundverständnis beitragen.

Viel Spass bei der Lektüre

Marco S. Meier, RA, MLaw, CIPP/E
Herausgeber

# Datenschutzrechtliche Haftung der Geschäftsleitung und des Verwaltungsrats

Mit dem revidierten Datenschutzgesetz (DSG) der Schweiz wurden neue Strafbestimmungen eingeführt. Um der Datenschutz-Compliance die nötige Aufmerksamkeit zu verschaffen, richten sich die Strafnormen nicht gegen Unternehmen, sondern explizit gegen natürliche Personen. Im Fokus stehen insbesondere Führungspersonen wie die Geschäftsleitung (GL) und der Verwaltungsrat (VR), aber auch Datenschutzbeauftragte. Ziel dieses Beitrags ist es, die datenschutzrechtliche Verantwortung von GL und VR zu beleuchten. Dabei werden straf- und zivilrechtliche Haftungsgrundlagen sowie die Voraussetzungen einer Haftung dargestellt. Zudem werden haftungspflichtige Personengruppen identifiziert, erste Praxisfälle aufgezeigt und abschliessend Empfehlungen formuliert.

**Von Eleonor Gyr**

## Haftungsgrundlagen im DSG

Grundsätzlich unterscheiden wir zwischen strafrechtlicher und zivilrechtlicher Haftung. Im DSG sind Strafbestimmungen verankert, bei denen natürliche Personen (und nicht das Unternehmen) bei gewissen Verletzungen gegen das DSG eine Strafverfolgung riskieren (siehe beispielsweise «Das Sanktionenregime des neuen Datenschutzgesetzes», WEKA Datenschutz Ausgabe 03, März 2023). Darüber hinaus können bei Verletzungen gegen das DSG aber auch weitere Straftatbestände, welche im Strafgesetzbuch (StGB) verankert sind, einschlägig sein, wie z. B. Berufsgeheimnisverletzung (Art. 321 StGB), oder Unbefugtes Beschaffen von Personendaten (Art. 179$^{novies}$). Auf diese Bestimmungen wird hier aber nicht näher eingegangen.

Im DSG sind Anspruchsgrundlagen von betroffenen Personen verankert, wie beispielsweise das Auskunftsrecht oder das Recht auf Datenherausgabe. Eine Verletzung dieser Ansprüche kann ggf. zu einer der vorerwähnten Strafsanktionen führen, so ist z. B. die vorsätzlich falsche oder unrichtige Auskunft mit Strafe bewehrt (Art. 60 DSG). Eine zivilrechtliche Haftungsnorm (Schadenersatz) enthält das DSG hingegen nicht direkt. Es gelten aber insbesondere die im Zivilgesetzbuch (ZGB) verankerten Persönlichkeitsrechte und die daraus abgeleiteten Ansprüche. Auch die im Aktienrecht verankerte Organhaftung könnte bei einer datenschutzrechtlichen Pflichtverletzung greifen. In Betracht kommt ebenfalls der ausservertragliche Haftungsanspruch von Art. 41 OR.

## Haftungsvoraussetzungen

Die strafrechtliche Verantwortlichkeit gemäss DSG setzt in der Regel einen Verstoss gegen eine explizit genannte Bestimmung des DSG, z. B. eine Verletzung der Informationspflicht, und vorsätzliches Handeln voraus. Vorsätzlich bedeutet, dass man mit Absicht (mit Wissen und Willen) gehandelt hat.

# Risikominimierende Massnahmen – Datenschutzerklärungen

Für Geschäftsleitungsmitglieder und Verwaltungsräte ist der richtige Umgang mit den Datenschutzerklärungen zentral zur Risikominimierung und zur Erfüllung ihrer Aufsichts- und Sorgfaltspflicht gemäss Datenschutzgesetz (DSG). Eine wirksame Datenschutzerklärung stellt ein zentrales Element eines umfassenden Datenschutzkonzepts dar. Sobald Personendaten beschafft werden, z. B. via Website, E-Mail, Formular, Bewerbungen, braucht die Unternehmung eine Datenschutzerklärung.

**Von Lukas Lezzi, Alexandra Egger**

**KEY TAKE-AWAYS**

**Inhalt der Datenschutzerklärung im Überblick**

- Kategorien und Herkunft der Daten
- Zwecke der Bearbeitung
- Rechtsgrundlagen (optional)
- Empfänger und Auftragsbearbeiter
- Auslandübermittlungen (inkl. Garantien)
- Schutz der Personendaten
- Dauer der Speicherung und Löschung
- Betroffenenrechte
- Kontakt für Datenschutzanliegen
- Änderungen dieser Datenschutzerklärung

## Anforderungen an die Datenschutzerklärung

Eine Datenschutzerklärung muss gewissen qualitativen Anforderungen entsprechen, um ihren Zweck zu erfüllen und rechtskonform zu sein. Die Datenschutzerklärung muss leicht zugänglich, verständlich, aktuell und transparent sein:

- leichte Zugänglichkeit:
  - Online-Publikation auf der Website
  - für Apps: Veröffentlichung innerhalb der App oder über einen externen Link
  - In E-Mails, Verträgen, Formularen etc. kann auf die Datenschutzerklärung verlinkt oder verwiesen werden.
  - für Offline-Geschäfte (z. B. Läden, Praxen): Die Datenschutzerklärung muss auf Wunsch ausgedruckt erhältlich sein.

  Ein Medienbruch liegt vor, wenn z. B. ein analoger Kontakt (z. B. via Telefongespräch) in eine digitale Datenbearbeitung überführt wird oder wenn über verschiedene Kanäle (z. B. physisch und digital) kommuniziert wird oder Daten erhoben werden. Gerade in diesen Fällen ist ein klarer Hinweis auf die Datenschutzerklärung notwendig. Ein Link auf Papier, wo die Datenschutzerklärung zu finden ist, reicht aus, sofern er zugänglich und eine gedruckte Version auf Anfrage erhältlich ist.
- Verständlichkeit: Die Datenschutzerklärung sollte in einer klaren, einfachen Sprache verfasst sein, die auch von juristischen Laien verstanden werden kann. Der Einsatz technischer oder juristischer Fachbegriffe sollte vermieden oder ausführlich erklärt werden.

  Die Datenschutzerklärung soll möglichst in der Sprache der Zielgruppe erhältlich sein (z. B. Deutsch, Französisch, Englisch).
- Aktualität: Die Datenschutzerklärung muss stets auf dem neuesten Stand gehalten werden. Werden neue Tools eingesetzt oder bestehende Prozesse geändert, müssen diese Änderungen in der Datenschutzerklärung reflektiert werden. Dies betrifft beispielsweise die Einbindung neuer Analyse-Tools oder die Nutzung eines anderen Newsletter-Dienstleisters.
- Transparenz gemäss Art. 19 DSG: Personen, deren Daten bearbeitet werden, müssen in geeigneter Weise über die Datenbearbeitung informiert werden (Details siehe unten).

  Werden Entscheidungen ausschliesslich automatisiert getroffen, die für die betroffene Person rechtliche Wirkungen entfalten oder sie erheblich beeinträchtigen, so ist dies in der Datenschutzerklärung offenzulegen. Zudem müssen Betroffene auf das Bestehen eines Rechts auf menschliches Eingreifen hingewiesen werden (Art. 21 DSG).
- Stellt die Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person dar (z. B. bei Überwachung öffentlicher Räume), sind zusätzliche Transparenzpflichten erforderlich. Das EDÖB und Datenschutzpraxis erwartet in solchen Fällen eine erhöhte inhaltliche Tiefe in der Datenschutzerklärung: z. B. genauere Angaben zu Algorithmen, Kriterien, Risiken, Speicherfristen sowie die Offenlegung besonderer Schutzmassnahmen.

  Zudem braucht es eine Datenschutz-Folgenabschätzung gemäss Art. 22 DSG. Diese muss folgende Punkte beinhalten:
  - Beschreibung der geplanten Bearbeitung
  - Bewertung der Risiken für die betroffene Person
  - Massnahmen zur Risikominderung (technisch und organisatorisch)
- In Fällen, in denen eine ausdrückliche Einwilligung für die Bearbeitung von Personendaten erforderlich ist (z. B. beim Versand von Werbung), muss die betroffene Person wissen, in welche Bearbeitung sie einwilligt.