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.

Die Datenschutzerklärung ist daher auch in diesem Fall zentral. Die Einwilligung muss dokumentiert und jederzeit abrufbar sein. Wichtig ist, dass keine globale Einwilligung in die Datenschutzerklärung verlangt wird, sondern nur in konkrete Bearbeitungstätigkeit.

- Die Datenschutzerklärung sollte idealerweise am Ende des internen Datenschutz-Governance-Prozesses erstellt werden. Dies bedeutet, dass vor der Erstellung und Veröffentlichung der Datenschutzerklärung klar definiert sein muss, welche Personendaten zu welchen Zwecken bearbeitet werden, wer Zugriff auf diese Daten hat und welche technischen und organisatorischen Massnahmen zum Schutz der Daten ergriffen werden. Nur auf dieser Grundlage kann eine transparente, vollständige und rechtskonforme Datenschutzerklärung ausgearbeitet werden.
- Datenschutzerklärungen sollten auch nie als Vertrag ausgestaltet oder in AGB einbezogen werden. Hierdurch würden nur unnötige vertragliche Risiken geschaffen.

Inhalt der Datenschutzerklärung

Die Datenschutzerklärung muss u. a. folgende Angaben enthalten:

- Die Datenschutzerklärung muss darlegen, welche Kategorien von Personendaten auf welchem Weg erhoben werden, z. B. Stammdaten (wie Name, Adresse, aus Kontaktformularen), Daten aus öffentlichen Registern (wie Strafregister, Grundbuch), Gesundheitsdaten aus Konsultationen.
- Zweck der Datenbearbeitung: Der Zweck muss konkret und verständlich formuliert sein. Es muss erklärt werden, weshalb die Daten erhoben, gespeichert und genutzt werden: z. B. Erfüllung eines Vertrags, Erfüllung gesetzlicher Pflichten, Marketing, Verbesserung von Dienstleistungen oder Produkten, Sicherheit.
- Rechtsgrundlagen der Bearbeitung: z. B. Vertrag, Einwilligung, berechtigtes Interesse.
- Einsatz von Cookies und Tracking-Technologien muss erläutert werden
- Zugriffsrechte und Datenweitergabe: Die Erklärung sollte klar benennen, welche Mitarbeitenden oder externen Dienstleister auf Personendaten zugreifen können (Empfänger und Kategorien von Empfängern wie Dienstleister, Behörden, Geschäftspartner, weitere Dritte wie Lieferadresse) und zu welchem Zweck eine Weitergabe erfolgt. Dabei ist auch zu differenzieren, ob es sich um Auftragsbearbeiter oder eigenständig Verantwortliche handelt. Ein Auftragsbearbeitungsvertrag (ABV) ist erforderlich, wenn ein Dritter im Auftrag des Verantwortlichen Personendaten bearbeitet. In der Datenschutzerklärung muss die Auftragsbearbeitung transparent erwähnt werden, wenn Personendaten durch Dritte im Auftrag bearbeitet werden.
- Übermittlung ins Ausland: Wenn Personendaten ins Ausland übermittelt werden, muss die Datenschutzerklärung Angaben über das Zielland, den Zweck der Übermittlung und die Schutzmassnahmen und Garantien machen. Falls kein angemessenes Datenschutzniveau besteht, sind Schutzmassnahmen wie Standardvertragsklauseln (SCC) oder Binding Corporate Rules zu nennen.
- Schutz der Personendaten: Die Datenschutzerklärung sollte nicht nur über die Datenbearbeitung informieren, sondern auch risikominimierende Massnahmen offenlegen, um Transparenz und Vertrauen zu fördern.
  - technische und organisatorische Massnahmen (TOMs): Dazu gehören z. B. Firewalls, Zugriffskontrollen, regelmässige Updates und Back-ups, Verschlüsselung der Kommunikation sowie die Trennung von besonders schützenswerten Daten.
  - organisatorische Massnahmen: interne Weisungen, Zugriffsregeln, Verpflichtung der Mitarbeitenden auf das Datengeheimnis, regelmässige Datenschutzschulungen sowie interne und externe Überprüfungen der Einhaltung der Datenschutzvorgaben.

- Dauer der Aufbewahrung/Löschung: Die Datenschutzerklärung sollte die Kriterien oder Fristen zur Aufbewahrung von Personendaten offenlegen. Zudem muss erklärt werden, wann und wie Daten gelöscht oder anonymisiert werden.
- Betroffenenrechte: Die Datenschutzerklärung muss die Rechte der Betroffenen aufzeigen: z. B. Auskunft, Berichtigung, Löschung, Widerspruch (z. B. gegen Direktmarketing) etc. Dies bedeutet auch, dass die Unternehmung Prozesse sicherstellen muss, welche z. B. regeln, wer für datenschutzrechtliche Anfragen zuständig ist oder wie mit Auskunftsbegehren umgegangen wird.
- Kontakt für Datenschutzanfragen
- Änderungen dieser Datenschutzerklärung

Haftung und Straffolge bei fehlender Transparenz

Art. 19 DSG verpflichtet Verantwortliche, betroffene Personen transparent über die Bearbeitung ihrer Personendaten zu informieren. Wer vorsätzlich also mit Wissen und Willen gegen Informationspflichten gemäss Art. 19 DSG verstösst, kann mit Busse bis zu CHF 250 000.– bestraft werden. Fahrlässigkeit ist nicht strafbar. Eine solche vorsätzliche Pflichtverletzung liegt z. B. vor, wenn eine Unternehmung Personendaten erhebt (z. B. Onlineformular), Tracking-Tools verwendet und der CEO mehrfach intern und extern auf die entsprechende Informationspflicht – welche über die Datenschutzerklärung erfolgt – hingewiesen wurde.

Gemäss Art. 754 OR haften Verwaltungsratsmitglieder persönlich, wenn sie ihre Pflichten verletzen und dadurch ein Schaden entsteht. Beispiel: Ein Unternehmen erhebt und bearbeitet Personendaten, verfügt aber über keine Datenschutzerklärung. Der VR ergreift trotz Kenntnis der entsprechenden Informationspflichten keine Massnahmen und delegiert diese nicht an eine Datenschutzbeauftragte. Nach einer Beschwerde eines Betroffenen beim EDÖB folgen Prüfung, negative Medienberichte und Kundenverlust. Eine zivilrechtliche Haftung des VR kann geprüft werden, z. B. wegen Reputations- oder Vermögensschäden, welche durch die Unternehmung geltend gemacht werden.

Fazit

Eine gut strukturierte, verständliche, aktuelle und einfach zugängliche Datenschutzerklärung ist ein wirksames Mittel zur Risikominimierung und zur Stärkung des Vertrauens bei betroffenen Personen. In Kombination mit technischen, organisatorischen und prozessualen Massnahmen bildet sie das Rückgrat eines effektiven Datenschutzkonzepts. Die Datenschutzerklärung sollte nicht als Vertrag oder Vertragsbestandteil ausgestaltet sein.

CHECKLISTE

1. Die Datenschutzerklärung muss aktuell, einfach verständlich (keine juristischen Fachbegriffe) und gut zugänglich sein.
2. Die Datenschutzerklärung sollte am Ende des internen Datenschutz-Governance-Prozesses erstellt werden. Zuerst muss definiert werden, welche Personendaten zu welchen Zwecken bearbeitet werden, wer Zugriff hat und welche Schutzmassnahmen nötig sind.
3. Die GL und der VR haben Organisationspflichten, worunter auch die Transparenzpflicht gemäss Art. 19 DSG fällt. Bei vorsätzlicher Verletzung dieser Pflicht kann es zur Haftung bzw. zu Straffolgen kommen.

AUTOREN

Lukas Lezzi ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.

Alexandra Egger arbeitet als Juristin bei LezziLegal. Sie arbeitet hauptsächlich im Bereich des Datenschutzrechts.