



### Datensicherheit ein Top-Down-Thema

In den meisten Umfragen zu den Prioritäten von Geschäftsführern für das Jahr 2025 rangiert das Thema «Datensicherheit» bzw. «Cybersecurity» auf den vordersten Plätzen. Der Hauptgrund dafür veranschaulicht ein Zitat von Serene Davis (Global Head of Cyber, QBE Insurance) «A breach alone is not a disaster, but mishandling it is.». Diese Aussage enthält zwei zentrale Punkte, nämlich, dass eine Verletzung der Datensicherheit jeden zu jederzeit treffen kann und, dass der Umgang mit einem solchen Vorfall zentral ist.

Gerade weil das Risiko hoch ist, dass ein Unternehmen von einem Datensicherheitsvorfall betroffen sein wird, ist die Vorbereitung darauf zentral, den die Folgen können gravierend sein. Das tönt auf den ersten Blick trivial, stellt Unternehmen aber vor grosse Herausforderungen. Wesentlich dabei ist, dass die Geschäftsleitung das Thema priorisiert und die Wichtigkeit hervorhebt. In der Praxis hat sich gezeigt, dass die Reaktion auf einen Datensicherheitsvorfall von der Geschäftsleitung und den ausgewählten Schlüsselfunktionen trainiert werden sollte. Aus datenschutzrechtlicher Sicht kann zudem eine Meldepflicht bei der zuständigen Behörde bestehen. Dazu hat der EDÖB kürzlich einen Leitfaden herausgegeben, der die rechtlichen Voraussetzungen behandelt.

Viel Spass bei der Lektüre

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

# Mindestvorgaben des DSG und praktische Umsetzung

Technologische Fortschritte eröffnen neue Chancen, bringen jedoch auch Herausforderungen und Risiken mit sich. Das Datenschutzgesetz (**DSG**) trägt dem Rechnung, indem es klare Anforderungen an die Datensicherheit stellt. Unternehmen sind verpflichtet, technische und organisatorische Massnahmen (**TOMs**) zu implementieren, um den Schutz von Personendaten sicherzustellen. Viele KMU stehen hier aber vor der Herausforderung, festzustellen, welche TOMs nun für ihr konkretes Geschäftsmodell im Sinne des Gesetzes nötig sind.

■ Von Dr. iur Lukas Lezzi

## Datensicherheit

Gemäss Art. 8 DSG sind Verantwortliche und Auftragsbearbeiter verpflichtet, angemessene TOMs zu ergreifen, um die Datensicherheit zu gewährleisten. Der Verantwortliche hat zudem sicherzustellen, dass der von ihm beauftragte Auftragsbearbeiter die erforderlichen Anforderungen erfüllt und über die nötigen TOMs verfügt.

## Mindestanforderungen an die Datensicherheit

Art. 1 Datenschutzverordnung (**DSV**), Art. 2 DSV und Art. 3 DSV bestimmen die Mindestanforderungen an die Datensicherheit. Die Mindestanforderungen agieren nicht als zwingende Massnahmen, sondern Kriterien, die zu berücksichtigen sind. Sie orientieren sich an den Grundsätzen der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit. Die Mindestanforderungen umfassen Folgendes:

### ■ Vertraulichkeit:

- Zugriffskontrolle: Personen dürfen nur auf Personendaten Zugriff haben, welche sie zur Erfüllung ihrer Aufgaben benötigen.
- Zugangskontrolle: Nur berechtigte Personen dürfen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden.

- Benutzerkontrolle: Unbefugte Personen dürfen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können.

### ■ Verfügbarkeit und Integrität:

- Datenträgerkontrolle: Unberechtigte Personen dürfen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten.
- Speicherkontrolle: Unberechtigte Personen dürfen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können.
- Transportkontrolle: Unberechtigte Personen dürfen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können.
- Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen muss bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.
- Systemsicherheit: Betriebssysteme und Anwendungssoftware müssen stets auf dem neuesten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden.

- Datenintegrität: Fehlfunktionen müssen gemeldet werden (Zuverlässigkeit), und gespeicherte Personendaten dürfen nicht durch Fehlfunktionen des Systems beschädigt werden können.

#### ■ **Nachvollziehbarkeit:**

- Eingabekontrolle: Es muss überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden.
- Bekanntgabekontrolle: Es muss überprüft werden können, wem Personendaten mithilfe von Einrichtungen zur Datenübertragung bekannt gegeben werden.
- Erkennung und Beseitigung: Verletzungen der Datensicherheit müssen rasch erkannt werden, damit Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können.

Die gesetzlichen Mindestvorschriften geben hier erst einmal die grundsätzlichen Bereiche und Themen vor, welche anhand der Sensibilität der Personendaten, dem Stand der Technik und den Implementierungskosten konkretisiert werden müssen. Dies geschieht im Unternehmen durch die TOMs.

### **Technische und organisatorische Massnahmen («TOMs»)**

Die TOMs müssen dem jeweiligen Risiko, welches die Datenbearbeitung für die betroffenen Personen mit sich bringt, angemessen sein. Dies bedeutet, dass ein risikobasierter Ansatz verfolgt werden muss. Dabei sind die Massnahmen nicht für alle Personendaten gleich auszugestalten, sondern müssen unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Datenbearbeitung an das jeweilige Risiko angepasst werden. Dabei sind die Prinzipien der Vertraulichkeit, Ver-

fügbareit, Integrität und Nachvollziehbarkeit zu wahren. Grundsätzlich gilt: Je sensibler die Personendaten, desto umfassender und strenger müssen die Massnahmen sein.

#### **Technische Massnahmen**

Unter technischen Massnahmen sind alle Vorkehrungen zu verstehen, die entweder technische Mittel zum Erreichen eines Schutzziels nutzen, integraler Bestandteil eines technischen Systems sind oder dem physischen Schutz dienen (z.B. ein Passwortschutz, Virens Scanner). Dies bedeutet, dass der Datenschutz bereits bei der Entwicklung eines neuen Projekts in Betracht gezogen werden soll. Dadurch soll sichergestellt werden, dass die Grundsätze des Datenschutzes durch Technik und Organisation eingehalten werden. Dementsprechend ist es nötig, die Datenbearbeitungsprozesse detailliert zu analysieren und ein Informationssicherheits- und Datenschutzkonzept auszuarbeiten. Folgende Punkte sollten als Standard implementiert werden:

- Zugriffskontrollen (z.B. Rollen- und Rechtekonzepte, Zwei-Faktor-Authentifizierung)
- Sicherung der Datenverfügbarkeit durch regelmässige Back-ups und Notfallpläne
- regelmässige Updates und Patches zur Behebung von Sicherheitslücken
- Schutzmechanismen wie Firewalls, VPN und Intrusion-Detection-Systeme
- Patch-Management (zur rechtzeitigen Einspeisung von Updates)
- geschützte Protokollierung
- Einsatz von Malware-/Virens Scannern
- Zutrittsbeschränkungen wie etwa Personenvereinzelnungsanlagen, Badge-Systeme, Iris Scanner etc.

Basierend auf den Risiken, welche eine Datenbearbeitung für die betroffenen Personen hat, sollten die folgenden weiteren Massnahmen in Betracht gezogen werden:

- Anonymisierung und Pseudonymisierung

- Verschlüsselung von Personendaten (z.B. bei Übertragung oder auf Speicherebene)
- Fähigkeit zur raschen Wiederherstellung der Verfügbarkeit von und des Zugriffs auf Personendaten
- Implementierung von intelligenten Bearbeitungs- und Löschfunktionen

Hervorzuheben ist, dass die Implementierungskosten nicht als Grund herangezogen werden können, um keine oder ungenügende Massnahmen zu implementieren.

Obwohl oft der Begriff «Verschlüsselung» verwendet wird, ist die Verschlüsselung von Personendaten – also die Umwandlung von Klartextdaten in ein unlesbares Format – weder im Ruhezustand noch bei der Übertragung von Daten zwingend erforderlich. Eine ähnliche Wirkung, ohne dass das Dateiformat geändert werden muss, kann auch durch Anonymisierung (ein Verfahren, bei dem Daten so verändert werden, dass kein Rückschluss mehr auf die betroffene Person möglich ist, wobei der Personenbezug mit angemessenem Aufwand nicht wiederhergestellt werden kann) oder Tokenisierung (bei der sensible Daten durch eindeutige Identifikationssymbole ersetzt werden, die alle wesentlichen Informationen über die Daten enthalten) erzielt werden.

#### **Organisatorische Massnahmen**

Organisatorische Massnahmen zielen auf das Umfeld des Systems, insbesondere die Personen, die es nutzen, ab. Sie legen Zuständigkeiten, Aufgaben und Verantwortlichkeiten im Bereich der Informationssicherheit fest und definieren Verhaltensrichtlinien für Mitarbeitende (z.B. interne Richtlinien, Schulungen, Empfehlungen). Auf organisatorischer Ebene sollten folgende Punkte beachtet werden:

- «Need-to-know»-Prinzip implementieren
- die Datenbearbeitung dokumentieren
- Schulungen und Sensibilisierung der Mitarbeitenden in Datenschutzfragen



## TOP 10 TOMS



- Need-to-know-Prinzip
- Einsatz von starken Passwörtern, Zwei-Faktor-Authentifizierung (2FA) und rollenbasierte Berechtigungen
- automatische Back-ups auf externen, sicheren Speichermedien oder in der Cloud
- Erstellung eines Wiederherstellungsplans
- Verschlüsselung sensibler Daten
- Verwendung von VPNs und verschlüsselten Kommunikationskanälen für externe Zugriffe
- regelmässige Schulungen zu Datenschutz, Phishing-Angriffen und sicheres Verhalten im Arbeitsalltag
- klare interne Richtlinien für den sicheren Umgang mit Personendaten und IT-Systemen
- automatische Updates für Betriebssysteme, Software und Sicherheitslösungen aktivieren
- sofortiges Schliessen von Sicherheitslücken

- strikte Clean Desk Policy
- Auftragsbearbeitungsverträge mit Dritten, die Zugang zu den Daten haben, abschliessen

## Protokollierung

Art. 4 DSV verlangt in bestimmten Situationen die Protokollierung von Datenbearbeitungen. Ziel dieser Protokollierung ist es, sicherheitsrelevante Ereignisse zu erfassen, die entsprechenden Daten zu speichern und sie für eine spätere Auswertung bereitzustellen. Als Massnahme der Datensicherheit im weiteren Sinne dient die Protokollierung sowohl der präventiven Erkennung von Sicherheitsvorfällen als auch der nachträglichen Analyse von Datenschutzverletzungen. Sie trägt zur Erreichung des Schutzziels der Nachvollziehbarkeit bei (Art. 2 Abs. 1 lit. d DSV) und ergänzt die Massnahmen gemäss Art. 3 Abs. 3 DSV. In Fällen, in denen eine Protokollierung gesetzlich vorgeschrieben ist, zählt sie zu den Mindestanforderungen der Datensicherheit.

Verantwortliche und Auftragsbearbeiter sind zur Protokollierung verpflichtet, wenn besonders schützenswerte Personendaten in grossem Umfang und auf automatisierte Weise bearbeitet werden. Zusätzlich muss eine Protokollierung erfolgen, wenn ein Profiling mit hohem Risiko durchgeführt wird. Verantwortliche und Auf-

tragsbearbeiter sind verpflichtet, mindestens die Vorgänge des Speicherns, Veränderns, Lesens, Bekanntgebens, Löschsens und Vernichtens von Daten zu protokollieren. Die Protokolle sind während mindestens einem Jahr getrennt vom System, in welchem die Personendaten bearbeitet werden, aufzubewahren (vgl. Art. 4 Abs. 5 DSV).

## Fazit

Unternehmen müssen angemessene TOMs implementieren, die sich an den spezifischen Risiken der Datenbearbeitung orientieren. Dabei sind Prinzipien wie Vertraulichkeit, Integrität und Nachvollziehbarkeit essenziell. Die Mindestanforderungen gemäss DSGVO und DSV bieten einen Rahmen für die Massnahmen, lassen jedoch genügend Spielraum für eine risikobasierte Anpassung. Unternehmen sollten den Datenschutz nicht als einmalige Massnahme, sondern als kontinuierlichen Prozess begreifen, der durch klare Verantwortlichkeiten, regelmässige Überprüfung und Anpassung an neue Entwicklungen getragen wird. Eine strategische und praxisnahe Umsetzung dieser Vorgaben ist entscheidend für eine nachhaltige Compliance.

## Zusammenfassung

- Unternehmen sind verpflichtet, angemessene technische und organisatorische Massnahmen (TOMs) umzusetzen, um die Sicherheit von

Personendaten zu gewährleisten. Die Mindestanforderungen des DSGVO und der DSV bieten einen Rahmen, müssen aber risikobasiert an das Unternehmen angepasst werden.

- Datenschutz erfordert eine Kombination aus technischen Sicherheitsvorkehrungen, organisatorischen Prozessen und Sensibilisierung der Mitarbeitenden. Besonders wichtige TOMs für KMU sind Zugriffskontrollen, Verschlüsselung, regelmässige Back-ups, Schulungen und Sicherheitsupdates.
- Datenschutz ist ein kontinuierlicher Prozess und keine einmalige Massnahme. Unternehmen müssen ihre Sicherheitsvorkehrungen regelmässig überprüfen, an neue Bedrohungen anpassen und eine nachhaltige Compliance-Strategie verfolgen.

## AUTOR



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