WEKA Business Dossier

Datenschutz im Gesundheitswesen

Rechtliche Rahmenbedingungen und Umsetzung in Gesundheitsorganisationen

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 im Gesundheitswesen

Projektleitung: Ina Görke
Satz: Sarah Rutschmann
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

DL8128-2155-202407

VLB – Titelaufnahme im Verzeichnis Lieferbarer Bücher:

© WEKA Business Media AG, Zürich
Alle Rechte, insbesondere das Recht auf Vervielfältigung und der Verbreitung sowie der Übersetzung, sind vorbehalten. Kein Teil des Werks darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung des Verlages reproduziert oder unter Verwendung elektronischer Systeme gespeichert, verarbeitet oder verbreitet werden. Wenn möglich verwenden wir immer geschlechtsneutrale Bezeichnungen. Aus Platzgründen oder aufgrund einer besseren Lesbarkeit verwenden wir bei Texten nur eine Schreibweise.

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 Organisations-Governance einzubeziehen.

Gesundheitsorganisationen 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 Richtlinien, Prozessen und Strukturen zu verstehen, weil das Thema Datenschutz in praktisch allen Aspekten einer Organisation zu berücksichtigen ist.

Das vorliegende Dossier hat zum Ziel, Gesundheitsorganisationen 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 die Organisation 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 in der Gesundheitsorganisation

Es ist in jedem Fall für die Umsetzung des DSG empfehlenswert, in der Praxis 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 die Praxis, 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 einer Gesundheitsorganisation als Stakeholder in einem solchen Projekt involviert sein, weil der Datenschutz letztlich alle Teile einer Organisation 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 Gesundheitspraxen 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 organisationsintern 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 der Organisation 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 Vorlaufzeit, 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.

3. Datenbearbeitungsgrundsätze

Das DSG geht davon aus, dass eine Datenbearbeitung zulässig ist, wenn die Bearbeitungsgrundsätze eingehalten werden und die Bearbeitung nicht gegen den ausdrücklichen Willen der betroffenen Person geschieht.

Folgende Bearbeitungsgrundsätze sind in Art. 6 DSG festgehalten und werden nachstehend erläutert:

- die Rechtmässigkeit
- Treu und Glauben und Transparenz
- die Verhältnismässigkeit
- die Zweckbindung
- die Richtigkeit

Alle Personendaten dürfen nur im Einklang mit den nachstehenden Grundsätzen bearbeitet werden. Wenn diese Grundsätze nicht vollständig eingehalten werden können, ist **eine** der folgenden Rechtfertigungen erforderlich (Art. 31 Abs. 1 DSG):

- die Einwilligung der betroffenen Person
- ein überwiegendes privates oder öffentliches Interesse oder
- eine gesetzliche Bestimmung

Eine Einwilligung in die Datenbearbeitung ist bei Einhaltung der Grundsätze selbst bei besonders schützenswerten Personendaten in der Regel nicht nötig. Ausnahme ist die Bekanntgabe von solchen Daten an Dritte.

3.1 Rechtmässigkeit

Wenn Personendaten nicht rechtmässig bearbeitet werden, stellt dies eine Verletzung der Persönlichkeit der betroffenen Person dar. Dies ist z. B. dann der Fall, wenn die Daten gegen den ausdrücklichen Willen der betroffenen Personen ohne Rechtfertigungsgrund bearbeitet werden oder wenn z. B. nicht alle Bearbeitungen in der Datenschutzerklärung offengelegt wurden.

3.2 Treu und Glauben und Transparenz

Die Datenbearbeitungen müssen den Grundsatz von Treu und Glauben und Transparenz berücksichtigen. Dies bedeutet insbesondere, dass die Sichtweise der betroffenen Person berücksichtigt werden muss. So verstösst eine Datenbearbeitung, mit der die betroffene Person nicht rechnen muss oder welche heimlich erfolgt, gegen den Grundsatz von Treu und Glauben. Die Anforderungen an die Transparenz der Datenbearbeitungen bedingen somit, dass betroffene Personen darüber informiert werden, wo welche Personendaten und zu welchem Zweck diese beschafft werden.

Die Organisation, die als für die Bearbeitung Verantwortlicher auftritt, muss die betroffenen Personen über bestimmte Umstände der Datenbearbeitung informieren, wenn es Daten über sie erhebt (z. B. in Form einer Datenschutzerklärung).

Das Transparenzprinzip verlangt darüber hinaus, dass alle Informationen und Mitteilungen über die Datenbearbeitung für die betroffenen Personen leicht zugänglich sowie klar und verständlich formuliert sein müssen. Sowohl die Datenbeschaffung als auch der Bearbeitungszweck müssen für die betroffene Person klar erkennbar sein.

In aller Regel genügt es, wenn auf der Webseite eine Datenschutzerklärung aufgeschaltet wird, welche für Besucher der Webseite, Kunden und Mitarbeitende von Dienstleistern gilt.

3.3 Verhältnismässigkeit

Eine Datenbearbeitung ist verhältnismässig, wenn die bearbeiteten Daten geeignet sind, den verfolgten Zweck zu erreichen, und dabei nur Daten bearbeitet werden, die hierzu auch erforderlich sind. Sie sind darüber hinaus zu vernichten, wenn sie gar nicht mehr benötigt werden (Art. 6 Abs. 4 DSG). Zu beachten ist, dass gesetzliche Aufbewahrungspflichten und berechtigte Interessen der Organisation vorbehalten bleiben.

3.4 Zweckbindung

Das Prinzip der Zweckbindung setzt voraus, dass der Zweck bei der Datenbeschaffung bereits konkretisiert sein muss und die weitere Bearbeitung der Daten sich an diesem Zweck ausrichtet.

Beschaffung und Bearbeitung von Personendaten dürfen nur für festgelegte und rechtmässige Zwecke erfolgen. Bereits bei der Datenbeschaffung muss der Zweck konkretisiert sein, und anschliessende Bearbeitungen müssen sich an diesem Zweck orientieren. Vage, undefinierte oder unpräzise Bearbeitungszwecke reichen nicht aus. Es dürfen nicht Personendaten nachträglich für Zwecke bearbeitet werden, die mit dem ursprünglichen Zweck nicht vereinbar sind. Dies schliesst jedoch nicht aus, dass personenbezogene Daten für andere Zwecke verwendet werden können, sofern hierfür eine Rechtsgrundlage oder Rechtfertigung vorliegt.

3.5 Richtigkeit

Bei dem Grundsatz der Richtigkeit handelt es sich um einen Aspekt der Datenqualität.

Die Anforderungen an die Richtigkeit der Daten müssen zweckorientiert ausgelegt werden. Je höher die Risiken für Persönlichkeitsrechte einer betroffenen Person sind, desto höhere Anforderungen sind an die Integrität zu stellen. Das heisst, desto mehr Aufwand muss getätigt werden, um die Korrektheit der Daten sicherzustellen, z. B. können bei einem Newsletter-Versand nicht aktuelle E-Mail-Adressen jeweils entfernt werden. Besonders schützenswerte Personendaten sollten hingegen aktiv regelmässig aktualisiert werden.