KANTON
LUZERN

Kantonale Datenschutzbeauftragte
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 61 00
datenschutz@lu.ch
www.datenschutz.lu.ch

Luzern, 22. Juli 2025

Merkblatt: Besonders schützenswerte Personendaten

Art. 13 Bundesverfassung (BV)

1 Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

2 Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

1 Personendaten

1.1 Was sind Personendaten?

Personendaten sind nach der gesetzlichen Definition alle Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (§ 2 Abs. 1 KDSG). Der Begriff ist sehr weit gefasst und umfasst nicht nur Angaben, die sich auf die persönlichen, sondern auch auf die sachlichen Verhältnisse einer Person beziehen (z. B. Angaben über ein Grundstück, die zu dessen Eigentümerschaft führen oder über ein immatrikuliertes Motorfahrzeug, die zu dessen Halter/in führen). Nicht als Personendaten (sog. Sachdaten) gelten nur solche Daten, die sich keiner individuellen Person zuordnen lassen. Bestimmt ist eine Person, wenn sie sich direkt aufgrund der Daten identifizieren lässt. Bestimmbar ist sie, wenn sie zwar nicht durch die fraglichen Daten allein, jedoch mit Hilfe anderer Informationen identifiziert werden kann. Erst dann, wenn der Aufwand zur Identifizierung unvernünftig gross wäre, gilt die Person nicht mehr als bestimmbar.

1.2 Was sind besonders schützenswerte Personendaten?

Aus den Personendaten wird rechtlich eine Unterkategorie ausgeschieden: Die besonders schützenswerten Personendaten.

Besonders schützenswerte Personendaten sind Daten, bei deren Bearbeitung eine besondere Gefahr einer Persönlichkeitsverletzung entsteht. Diese Gefahr kann aufgrund der Bedeutung der Daten, des Zusammenhangs, des Zwecks oder der Art der Bearbeitung, der Datenkategorie oder anderer Umstände entstehen.

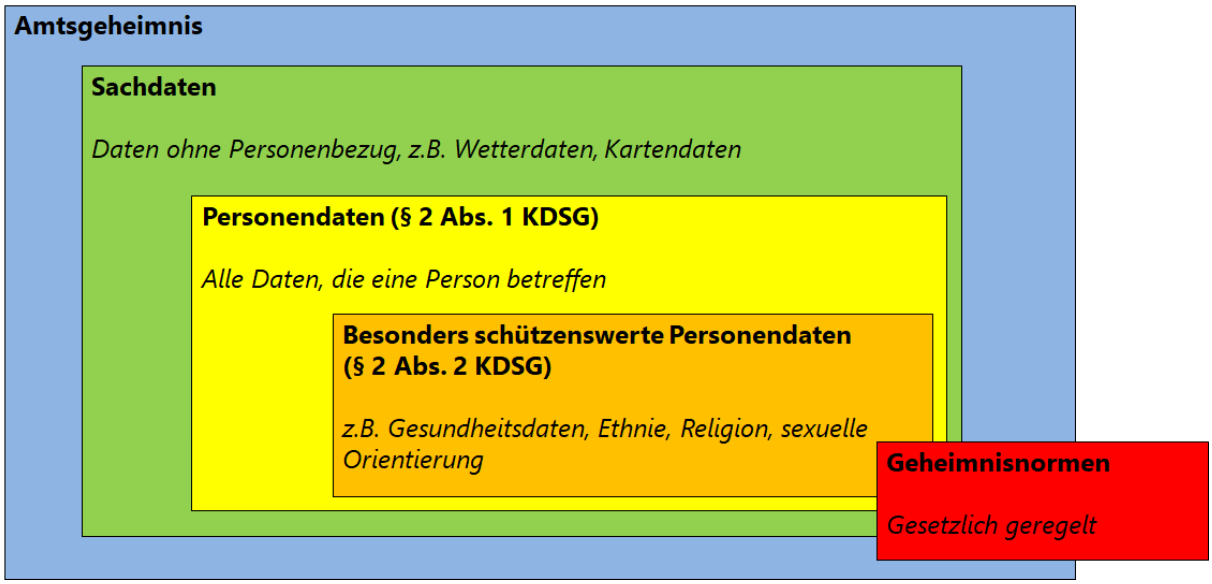
Als «normale» Personendaten und nicht dieser Kategorie zugehörig gelten daher im Umkehrschluss Angaben, die die Persönlichkeit nicht im innersten Kern tangieren und oft in irgendeiner Form allgemein zugänglich sind (z.B. Name, Adresse, Geburtsjahr, Zivilstand usw.).

Gemäss § 2 Abs. 2 KDSG sind besonders schützenswerte Personendaten Angaben über natürliche Personen, bei welchen eine besondere Gefahr für Persönlichkeits- und Grundrechtsverletzungen besteht, insbesondere:

a. Daten über die religiöse, weltanschauliche oder politische Haltung,
b. Daten über die Gesundheit, die Intimsphäre, das Erbgut oder die ethnische Zugehörigkeit,
c. mit speziellen technischen Verfahren gewonnene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten),
d. Daten über verwaltungs- und strafrechtliche Massnahmen und Sanktionen sowie Massnahmen der Sozialhilfe,
e. Zusammenstellungen von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person erlaubt (Persönlichkeitsprofil).

Diese Aufzählung ist nicht abschliessend. Es ist daher immer fallweise zu prüfen, ob eine besondere Gefahr einer Persönlichkeitsverletzung besteht. So sind beispielsweise Adressdaten nicht grundsätzlich besonders schützenswerte Personendaten. Dabei ist aber der Zusammenhang der Bearbeitung zu beachten. Gibt eine Einwohnerkontrolle Adressdaten einer Person bekannt, ist der Zusammenhang ein harmloserer als bei der Bekanntgabe von Adressdaten durch das Sozialamt, weil er den Bezug von Leistungen der sozialen Hilfe impliziert.

1.3 Zusammenfassung



Kurz erklärt:

***Amtsgeheimnis**:* *Die Geheimhaltungspflicht gilt für die gesamte kantonale Verwaltung (vgl. § 52 Personalgesetz).*

***Sachdaten**:* *Daten ohne direkten Personenbezug (z.B. Temperatur, Gebäudegrösse, Zusammensetzung von Medikament).*

***Personendaten**:* *Alle Daten, die sich auf eine identifizierbare Person beziehen (z.B. Name, Adresse).*

***Besonders schützenswerte Personendaten**:* *Eine Unterkategorie von Personendaten, die einen erhöhten Schutz benötigen (z.B. Gesundheitsdaten, politische Meinung, religiöse Überzeugungen).*

***Geheimnisnormen**:* *Geheimhaltungsverpflichtungen, die in Gesetzen geregelt sind (siehe dazu unten Ziff. 4).*

2 Bearbeiten von Personendaten - Legalitätsprinzip

Auch das «Bearbeiten» von Personendaten ist ein sehr weiter Begriff, der jeden Umgang mit Personendaten erfasst. Das Bearbeiten von Personendaten ist gemäss § 2 Abs. 4 KDSG, unabhängig von den angewendeten Mitteln und Verfahren, jeder Umgang mit Daten, wie das Erheben, Beschaffen, Aufbewahren, Aufzeichnen, Sammeln, Speichern auf elektronischen Datenträgern, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen und Vernichten.

Bekanntgeben ist das Übermitteln oder das Zugänglichmachen von Personendaten, insbesondere durch Einsichtgewähren, Weitergeben oder Veröffentlichen.

Gemäss § 5 Abs. 1 KDSG dürfen Organe Personendaten bearbeiten, wenn:

a. dafür eine Rechtsgrundlage besteht oder
b. dies zur Erfüllung von Aufgaben erforderlich ist, für die eine Rechtsgrundlage besteht.

Für jede Datenbearbeitung durch öffentliche Organe muss zwingend eine Rechtsgrundlage bestehen. Dies kann ein Gesetz, ein Dekret oder eine Verordnung sein. Auch kommunale Erlasse gelten als Rechtsgrundlagen. Es bedarf dabei nicht stets einer unmittelbaren, d. h. ausdrücklichen Rechtsgrundlage. So kann eine erforderliche, d. h. mehr als nur nützliche und wünschbare Datenbearbeitung grundsätzlich auch aus einer Bestimmung im Gesetz oder in der Verordnung, welche die Aufgaben des öffentlichen Organs umschreibt, abgeleitet werden.

Sollen hingegen **besonders schützenswerte Personendaten** bearbeitet werden, bedarf es einer ausdrücklichen **Grundlage in einem formellen Gesetz** oder die Datenbearbeitung muss zur **Erfüllung einer in einem formellen Gesetz umschriebenen gesetzlichen Aufgabe** unentbehrlich sein (§ 5 Abs. 2 lit. a und b KDSG). Die Anforderungen beim Bearbeiten besonders schützenswerter Personendaten sind erhöht, weil bei diesen eine besondere Gefahr von Persönlichkeitsverletzungen besteht.

3 Verantwortlichkeit

3.1 Allgemeines

Gemäss § 6 Abs. 1 KDSG ist für den Datenschutz jedes Organ verantwortlich, das Personendaten bearbeitet oder bearbeiten lässt.

Das verantwortliche Organ stellt mit technischen und organisatorischen Massnahmen die Einhaltung des Datenschutzes sicher. Die Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Rechte der betroffenen Personen mit sich bringt, angemessen sein (§ 6 Abs. 1bis KDSG).

Gemäss § 6 Abs. 3 KDSG kann das Bearbeiten von Personendaten einem anderen Organ oder Dritten übertragen (sog. Auftragsdatenbearbeitung), wenn:

a. keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht,
b. sichergestellt ist, dass die Personendaten nur so bearbeitet werden, wie es das verantwortliche Organ selbst tun dürfte; insbesondere darf das Bearbeiten von Personendaten nicht ohne vorgängige schriftliche Zustimmung des verantwortlichen Organs weiteren Auftragsdatenbearbeitern übertragen werden.

3.2 Verantwortlichkeit bei Datenbearbeitungen in der Cloud

Bei der Inanspruchnahme von Cloud-Lösungen von Drittanbietern bestehen oder akzentuieren sich Risiken in verschiedenen Bereichen. Das verantwortliche öffentliche Organ hat diese Risiken durch angemessene Massnahmen auszuschliessen oder auf ein tragbares Mass zu reduzieren**; ist dies nicht möglich, so ist auf die Cloud-Leistung zu verzichten**.

Bei der Risikoanalyse für die konkrete Datenbearbeitung sind die cloudspezifischen Risiken zu berücksichtigen und entsprechende Vorkehrungen zu treffen.

Im Vordergrund stehen fünf Risikobereiche:

- Vertragsgestaltung,
- Orte der Datenbearbeitungen einschliesslich ausländische Behördenzugriffe,
- Vertraulichkeit/Geheimnisschutz, Verschlüsselung und Schlüsselmanagement
- Daten über die Nutzerinnen und Nutzer der Cloud-Dienste und
- Unterauftragsverhältnisse.

Das cloudspezifische Risiko wird primär von diesen fünf Risiken bestimmt. Hinzu kommen weitere Risiken, die durch die Verwendung von Cloud-Infrastruktur mindestens akzentuiert werden: Meldepflichten, Kontrollrecht und -möglichkeit, Informationssicherheitsmassnahmen und Pflichten bei Vertragsauflösung.

Schliesslich ist auch zu berücksichtigen, dass sich die Abhängigkeiten vom Leistungserbringer (Verfügbarkeit, Migrationsaufwand bei Wechsel) weiter erhöhen.

➔ Vgl. Cloud-Merkblatt der Konferenz der schweizerischen Datenschutzbeauftragten (privatim)

4 Verhältnis gesetzliche Geheimhaltungspflicht besonders schützenswerte Personendaten

Beispiele für Gesetze mit Geheimhaltungspflichten sind:

- Amtsgeheimnis:
  Art. 320 StGB für Beamte und Behördenmitarbeiter
  ➔ § 52 Personalgesetz: Geheimhaltungspflicht gilt für die gesamte kantonale Verwaltung

- Sozialhilfe, Sozialversicherungen:
  Art. 33 ATSG, Art. 84 AHVG, Art. 62 IVG, usw.

- Opferhilfegesetz:
  Art. 11 OHG

- Bankgeheimnis:
  Art. 47 BankG

- Berufsgeheimnisse:
  Art. 321 StGB (Ärzte, Anwälte, Geistliche usw.)
  Art. 321bis StGB (Psychologen)

Diese gesetzlichen Geheimhaltungspflichten verbieten grundsätzlich die Offenlegung der anvertrauten Informationen, unabhängig davon, ob sie besonders schützenswerte Personendaten darstellen oder nicht. Sie gelten als lex specialis, also als spezialgesetzliche Vorschriften gegenüber dem allgemeinen Datenschutzrecht.

Das KDSG gilt zusätzlich zu spezialgesetzlichen Geheimhaltungsregeln. Die Einhaltung der besonderen Geheimhaltungspflicht entbindet nicht von der Pflicht, Datenschutzvorgaben einzuhalten. Umgekehrt vermag das Datenschutzrecht eine strengere Geheimhaltungspflicht nicht aufzuheben (vgl. dazu § 9 Abs. 1 KDSG).

Merke: Das Vorliegen einer Bearbeitung von besonders schützenswerten Personendaten ebenso wie jene von speziellen Geheimnisnormen ergibt sich aus dem Gesetz selbst und lässt sich nicht mit einer «Datenklassifizierung» übersteuern.

Postadresse:	Datenschutzbeauftragte des Kantons Luzern Bahnhofstrasse 15 6002 Luzern
Kontaktformular:	https://datenschutz.lu.ch/kontakt
Telefon:	+ 41 41 228 61 00
E-Mail:	datenschutz@lu.ch **WARNUNG**: Der E-Mail-Verkehr ist unsicher. Vertrauliches gehört deshalb nicht in E-Mails!
Website:	https://datenschutz.lu.ch/