

Art. 8 DSG: Datensicherheit

Funktion und Systematik

Art. 8 DSG verpflichtet den Verantwortlichen und den Auftragsbearbeiter, durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten (Abs. 1). Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden (Abs. 2). Der Bundesrat erlässt Mindestanforderungen (Abs. 3) **Art. 8 DSG**.

Nach der Botschaft kommt in Abs. 1 der risikobasierte Ansatz zum Ausdruck: «Je grösser das Risiko einer Verletzung der Datensicherheit, umso höher sind die Anforderungen an die zu treffenden Massnahmen.» **BBI 2017 6941**. Abs. 2 bestimmt nach derselben Quelle das Ziel der Massnahmen. Die Bestimmung stand bereits im bundesrätlichen Entwurf (Art. 7 E-DSG), der den früheren Art. 7 aDSG «mit einigen Änderungen» übernahm **BBI 2017 6941**. Seit dem Inkrafttreten am 1. September 2023 ist Art. 8 DSG unverändert geblieben. Weil die Bestimmung an Art. 7 aDSG anknüpft, bleibt die Rechtsprechung zum alten Recht als Auslegungshilfe verwertbar.

Die Botschaft grenzt Datensicherheit vom Datenschutz ab: «Beim Datenschutz geht es um den Persönlichkeitsschutz des Einzelnen.» Die Datensicherheit zielt «hingegen generell auf die bei einem Verantwortlichen oder Auftragsbearbeiter vorhandenen Daten ab und umfasst den allgemeinen technischen und organisatorischen Rahmen der Datenbearbeitung» **BBI 2017 6941**. Daraus folgt die Abgrenzung zu Art. 7 DSG (Datenschutz durch Technik). Dieser verlangt, die Bearbeitung so auszugestalten, dass die Datenschutzvorschriften, insbesondere die Grundsätze nach Art. 6, eingehalten werden, und richtet sich nur an den Verantwortlichen **Art. 7 DSG**. Art. 8 DSG schützt demgegenüber die Schutzziele der Daten selbst und bindet auch den Auftragsbearbeiter.

Normadressaten und Auftragsbearbeitung

Pflichtig sind der Verantwortliche und der Auftragsbearbeiter, jeweils als private Person oder als Bundesorgan (Art. 5 lit. j und k DSG) **Art. 5 DSG**. Der Auftragsbearbeiter trägt damit eine eigene Sicherheitspflicht, die nicht bloss vom Verantwortlichen abgeleitet ist. Ergänzend muss sich der Verantwortliche nach Art. 9 Abs. 2 DSG «insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten». Unteraufträge bedürfen der vorgängigen Genehmigung des Verantwortlichen (Art. 9 Abs. 3 DSG) **Art. 9 DSG**. Diese Auswahlpflicht ist strafrechtlich abgesichert: Wer vorsätzlich die Bearbeitung einem Auftragsbearbeiter übergibt, ohne dass die Voraussetzungen von Art. 9 Abs. 1 und 2 DSG erfüllt sind, wird nach Art. 61 lit. b DSG gebüsst **Art. 61 DSG**. Das Obergericht Zürich behandelt diesen Tatbestand als mit der Übergabe vollendet und nicht als Dauerdelikt. Der weitere Besitz der Daten beim Empfänger verlängert die Verjährung deshalb nicht **UE240022**. Das Kantonsgericht Schwyz hob eine Nichtanhandnahme zu Art. 61 lit. b DSG auf, weil die Staatsanwaltschaft eine mögliche gesetzliche Geheimhaltungspflicht (Art. 9 Abs. 1 lit. b DSG) nicht geprüft hatte. Eine Nichtanhandnahme dürfe nur bei «offensichtlicher Straflosigkeit» ergehen **BEK 2024 84**. In seiner Aufsichtspraxis (Fälle Xplain und Concevis) verlangt der EDÖB, dass Verträge mit Auftragsbearbeitern den Datenlebenszyklus präzise festlegen und Kontrollen und Audits

klar regeln **EDÖB 32. Tätigkeitsbericht 2024/2025** Diese Praxis ist nicht verbindlich, zeigt aber, wie die Aufsicht die Vergewisserungspflicht nach Art. 9 Abs. 2 DSG versteht.

Geltungsbereich: Abgrenzung zu kantonalen Organen

Das DSG gilt nur für private Personen und Bundesorgane. Ausgenommen sind unter anderem Bearbeitungen ausschliesslich zum persönlichen Gebrauch sowie Bearbeitungen durch die eidgenössischen Räte und Kommissionen im Rahmen ihrer Beratungen (Art. 2 Abs. 1 und 2 DSG) **Art. 2 DSG**. Kantonale und kommunale Organe unterstehen nach dem Bundesgericht nicht dem DSG, und zwar «même s'ils sont chargés de l'exécution de tâches de la Confédération» (auch wenn sie mit dem Vollzug von Bundesaufgaben betraut sind). Für die IV-Stelle Waadt galt deshalb das kantonale Datenschutzgesetz **1C_125/2015**. Für solche Organe gelten die Sicherheitsbestimmungen des kantonalen Rechts. Das Genfer Recht etwa verlangt in Art. 37 LIPAD geeignete organisatorische und technische Massnahmen gegen jede unrechtmässige Bearbeitung **ATA/663/2024**. Auch Private können als kantonale Organe gelten, etwa wenn sie aufgrund eines Leistungsauftrags tätig sind oder überwiegend öffentlich finanziert werden. Die Aufsicht liegt dann bei den kantonalen Behörden; die Zuordnung ist im Einzelfall zu prüfen **150007355**. Diese Stellungnahme des Bundesamts für Justiz ist eine Verwaltungsmeinung, keine gerichtliche Entscheidung.

Verletzung der Datensicherheit und Massnahmenpflicht

Die Legaldefinition in Art. 5 lit. h DSG erfasst eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden **Art. 5 DSG**. Nach der Botschaft wurde die Bestimmung zur Datensicherheit präzisiert, «weil ihr Anwendungsbereich sehr unklar schien» **BBI 2017 6941**.

Das Bundesverwaltungsgericht beschreibt die Verletzung als «planwidrigen Vorfall mit Sicherheitsrelevanz». Es hält fest: «Ob sich eine Verletzung der Datensicherheit ereignet hat, ist unabhängig davon zu beurteilen, ob diese schuldhaft oder widerrechtlich herbeigeführt wurde.» **a-3790-2024**. Im Fall konnte ein Suchmaschinen-Crawler kundenbezogene URLs indexieren, was das Gericht als «Konfiguration- oder Sicherheitsproblem» des Verantwortlichen qualifizierte. Nachträgliche technische Sperren vermochten «eine bereits erfolgte unbefugte Offenlegung nicht rückwirkend zu beseitigen» **a-3790-2024**.

Daraus folgt eine wichtige Unterscheidung. Der Begriff der Verletzung ist verschuldensunabhängig und knüpft an den Erfolg an. Art. 8 DSG begründet dagegen eine Massnahmenpflicht: Die Massnahmen müssen Verletzungen vermeiden «ermöglichen» (Abs. 2) **Art. 8 DSG**. Ein Vorfall beweist deshalb nicht für sich, dass Art. 8 DSG verletzt wurde. Das Bundesgericht hat noch unter altem Recht festgehalten: «Geschuldet ist kein absoluter Schutz» **BGE 144 I 126**. Der Erläuternde Bericht zur DSV sagt ebenso: «Eine absolute Sicherheit kann und soll nicht verlangt werden.»

EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) - A-3790/2024 äussert sich zum Verhältnis zwischen Vorfall und

Pflichtverletzung nach Art. 8 DSGVO allerdings nicht ausdrücklich; der Entscheid betrifft die Informationspflicht nach Art. 24 DSGVO (dazu unten).

Der risikobasierte Massstab: Schutzbedarf, Risiko, Stand der Technik und Kosten

Art. 1 DSGVO konkretisiert Abs. 1 in zwei Schritten. Zuerst ist der Schutzbedarf der Daten zu bestimmen, und zwar nach der Art der Daten sowie nach Zweck, Art, Umfang und Umständen der Bearbeitung (Abs. 2). Danach ist das Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zu beurteilen. Massgebend sind die Ursachen des Risikos, die hauptsächlichen Gefahren, die ergriffenen oder vorgesehenen Massnahmen sowie Wahrscheinlichkeit und Schwere einer Verletzung trotz dieser Massnahmen (Abs. 3). Bei der Wahl der Massnahmen sind zusätzlich der Stand der Technik und die Implementierungskosten zu berücksichtigen (Abs. 4). Die Pflicht dauert an: Schutzbedarf, Risiko und Massnahmen sind «über die gesamte Bearbeitungsdauer hinweg zu überprüfen», und die Massnahmen sind nötigenfalls anzupassen (Abs. 5) **Art. 1 DSGVO**.

Stand der Technik und Implementierungskosten begrenzen den Pflichtumfang nur innerhalb des Angemessenen. Nach dem Erläuternden Bericht genügt es, Massnahmen zu treffen, «die bereits zur Verfügung stehen und sich entsprechend bewährt haben». Kosten umfassen auch personelle und zeitliche Ressourcen. Der Verantwortliche kann sich aber «nicht mit der Begründung von der Pflicht einer angemessenen Datensicherheit befreien, dass damit übermässige Kosten verbunden sind»

EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV), Erläuternder Bericht

. Kosten bestimmen also, welches Mittel gewählt wird, nicht ob überhaupt Massnahmen getroffen werden. Der Bericht ist eine Verwaltungserläuterung; er bindet die Gerichte nicht, deckt sich aber mit dem Wortlaut von Art. 8 Abs. 1 DSGVO.

Verbindliche technische Normen schreibt das Recht nicht vor. Die III. Strafkammer des Obergerichts Zürich hielt fest: «Das Datenschutzgesetz und die Datenschutzverordnung enthalten keine verbindlichen Vorgaben für Daten- bzw. Informationssicherheitsstandards.» **UE240472**. Für eine E-Mail mit Finanz- und Adressdaten genügte deshalb eine erzwungene TLS-Transportverschlüsselung. Die Forderung nach Ende-zu-Ende-Verschlüsselung wies das Gericht zurück, auch weil solche Daten nicht zu den besonders schützenswerten Daten gehören **UE240472**. Der Entscheid erging in einem Strafverfahren (Nichtanhandnahme) und ist deshalb vorsichtig auf den zivil- oder aufsichtsrechtlichen Massstab zu übertragen. Strenger fällt die Beurteilung bei hohem Schutzbedarf aus: Für Telekommunikations-Randdaten stellte das Bundesgericht darauf ab, dass die Übermittlung nur durch vorgängig authentifiziertes Personal und verschlüsselt erfolgt und der Systemzugang auf registrierte und überprüfte Nutzer beschränkt ist **BGE 144 I 126**.

Die kantonale Praxis wendet denselben Verhältnismässigkeitsgedanken an. Das Verwaltungsgericht Bern stellte für eine kantonale Geschäftsverwaltungssoftware darauf ab, dass sich die erforderlichen Massnahmen nach dem Grundsatz der Verhältnismässigkeit und den konkreten Risiken beurteilen. Über die gerügte fehlende Zwei-Faktoren-Authentifizierung entschied es mangels aktuellen Interesses aber nicht **100 2017 72**. Das Kantonsgericht Waadt verlangte bei einer Videoüberwachung eine manuelle Protokollierung der Zugriffe auf die Aufnahmen. Es hielt aber fest: «il serait toutefois disproportionné d'exiger le renouvellement des installations pour ce seul motif» (es wäre jedoch unverhältnismässig, allein aus diesem Grund die Erneuerung der Anlagen zu verlangen) **ge-2012-0139**. Beide Entscheide ergingen nach kantonalem Recht und sind für Art. 8 DSGVO nur als Analogie verwertbar.

Schutzziele und Massnahmenkatalog

Art. 2 DSGVO nennt vier Schutzziele: Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit **Art. 2 DSGVO**. Art. 3 DSGVO ordnet ihnen Massnahmen zu. Zur Vertraulichkeit gehören Zugriffs-, Zugangs- und Benutzerkontrolle. Zu Verfügbarkeit und Integrität gehören Datenträger-, Speicher- und Transportkontrolle, Wiederherstellung, Zuverlässigkeit und Systemsicherheit, wozu auch das Schliessen bekannter kritischer Lücken zählt. Zur Nachvollziehbarkeit gehören Eingabe- und Bekanntgabekontrolle sowie die rasche Erkennung und Beseitigung von Verletzungen **Art. 3 DSGVO**. Die Massnahmen sind «ihrem Schutzbedarf entsprechend» zu treffen **Art. 2 DSGVO**. Der Katalog ist deshalb ein Prüfraster und keine Liste, die in jedem Fall vollständig umgesetzt werden muss.

Zugriffskontrolle und need-to-know. Den Grundsatz, dass berechtigte Personen nur auf die Daten zugreifen dürfen, die sie für ihre Aufgaben benötigen (heute Art. 3 Abs. 1 lit. a DSGVO), wandte das Bundesverwaltungsgericht schon unter altem Recht an. Eine Vorsorgeeinrichtung versandte Pensionskassenausweise in unverschlossenen Couverts an die Arbeitgeber zur Weiterleitung. Das verletzte den Grundsatz der Datensicherheit nach Art. 7 aDSG, weil die Arbeitgeber die individuelle Vorsorgesituation nicht kennen müssen. Das Gericht verlangte den Direktversand oder zumindest verschlossene, namentlich adressierte und als vertraulich bezeichnete Couverts **a-4467-2011**. Der Entscheid zeigt, dass auch einfache organisatorische Massnahmen geschuldet sein können.

Spitäler und Patientendossiers. Die Genfer Chambre administrative wies einen Zugriffsmangel als rechtmässig, das den Zugriff nach Profil, Tätigkeitszone und Zeitfenster der Behandlung begrenzt. Für Notfälle besteht ein begründungspflichtiger Ausnahmезugriff («vitre brisée»), und alle Zugriffe werden protokolliert und nachträglich kontrolliert. Unzulässig war hingegen der Zugriff einer Ärztin, die den Patienten nicht behandelte und sich wahrheitswidrig als zuständig ausgab **ATA/663/2024**. Der Fall trennt das Systemdesign, das genügte, vom missbräuchlichen Einzelzugriff, der eine Persönlichkeitsverletzung darstellte. Die Genfer Chambre pénale de recours sah im Zugriff des Abrechnungspersonals einer Klinik auf das medizinische Dossier keine offenkundige Verletzung der Mindestanforderungen. Dieses Personal benötigte den Zugriff für die Fakturierung und untersteht ebenfalls dem Berufsgeheimnis. Die Frage der Verhältnismässigkeit der Zugriffsorganisation sei im Wesentlichen zivilrechtlich **ACPR/239/2025**.

Videoüberwachung und Zugriffskreise. Das Kantonsgericht Freiburg beanstandete ein kommunales Videoreglement, weil der Kreis der Zugriffsberechtigten «trop étendu et trop imprécis» (zu weit und zu unbestimmt) war und weil ein Passwortschutz allein für die Sicherheit der Daten nicht genügt **601 2014 46**.

Fehlende formelle Sicherheitsprüfung. Das Bundesverwaltungsgericht liess einen Smart Meter übergangsrechtlich weiter zu, obwohl die spezialgesetzliche Datensicherheitsprüfung nach Art. 8b StromVV fehlte. Der Netzbetreiber bleibt aber an die materiellen Sicherheitsanforderungen gebunden, und es fehlten konkrete Hinweise auf eine unsichere Bearbeitung **a-2372-2021**. Für die Rüge einer Verletzung der Datensicherheit verlangt der Entscheid also konkrete Anhaltspunkte.

Protokollierung und Bearbeitungsreglement

Art. 4 DSGVO in der seit 1. Dezember 2025 geltenden Fassung regelt die Protokollierung. Private Verantwortliche und ihre privaten Auftragsbearbeiter müssen protokollieren, wenn besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird und die präventiven Massnahmen den Datenschutz nicht gewährleisten können. Zu protokollieren sind mindestens das Speichern, Verändern, Bekanntgeben, Löschen und Vernichten sowie

das Zugreifen. Bundesorgane müssen in bestimmten Fällen immer protokollieren. Bei den übrigen automatisierten Bearbeitungen entscheiden sie aufgrund einer vorgängigen, schriftlichen Risikobeurteilung, ob und in welchem Umfang sie protokollieren. Diese Beurteilung ist dem EDÖB auf Anfrage mitzuteilen (Abs. 2 und 2bis). Die Protokolle sind mindestens ein Jahr getrennt vom Produktivsystem aufzubewahren und dürfen nur für Kontroll- und Sicherheitszwecke verwendet werden (Abs. 5) **Art. 4 DSV**. Für Bearbeitungen von Bundesorganen, die vor der Änderung geplant oder begonnen wurden, ist die Prüfung bis 31. Dezember 2026 vorzunehmen. Eine nötige Protokollierung ist bis 31. Dezember 2029 zu implementieren; davon ausgenommen sind die Fälle, in denen ohnehin protokolliert werden muss **Art. 46 DSV**.

Die Zweckbindung der Protokolle hat praktisches Gewicht. Die Genfer Chambre administrative hielt nach kantonalem Recht fest, dass Badge-Zutrittsprotokolle, die für die Sicherheit der Räume erhoben wurden, nicht zur Arbeitszeitkontrolle verwendet werden dürfen. Sie ordnete die Vernichtung der entsprechenden Dateien an **ATA/1316/2024**. Das entspricht der Zweckbindung, die Art. 4 Abs. 5 DSV bundesrechtlich ausdrücklich vorsieht **Art. 4 DSV**.

Ein Bearbeitungsreglement für automatisierte Bearbeitungen müssen Private erstellen, wenn sie besonders schützenswerte Personendaten in grossem Umfang bearbeiten oder ein Profiling mit hohem Risiko durchführen. Es muss namentlich die interne Organisation, das Bearbeitungs- und Kontrollverfahren und die Sicherheitsmassnahmen beschreiben und regelmässig aktualisiert werden **Art. 5 DSV**. Für Bundesorgane ist der Katalog breiter. Er umfasst unter anderem jede Bearbeitung besonders schützenswerter Daten, jedes Profiling, das Zugänglichmachen an Dritte und die Verknüpfung von Datenbeständen **Art. 6 DSV**. Ein solches Reglement kann sicherheitsrelevante Angaben enthalten, etwa zu Benutzer- und Zugriffsrechten und zur Datensicherheit. Beim Reglement des Nachrichtendienstes des Bundes war deshalb der Zugang nach dem Öffentlichkeitsgesetz aufgrund des Spezialgesetzes ausgeschlossen **a-4286-2022**.

Meldung und Information nach einer Verletzung

Art. 8 DSG wirkt präventiv. Art. 24 DSG regelt, was nach einem Vorfall geschieht. Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung, die voraussichtlich zu einem hohen Risiko für die betroffene Person führt. Der Auftragsbearbeiter meldet dem Verantwortlichen jede Verletzung. Betroffene sind zu informieren, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt (Abs. 1, 3 und 4). Eine Meldung darf im Strafverfahren gegen die meldepflichtige Person nur mit deren Einverständnis verwendet werden (Abs. 6). Seit 1. April 2025 kann der EDÖB die Meldung mit Einverständnis des Verantwortlichen an das Bundesamt für Cybersicherheit weiterleiten (Abs. 5bis) **Art. 24 DSG**. Art. 15 DSV legt den Mindestinhalt der Meldung fest. Er verlangt zudem, dass jede Verletzung mit Tatsachen, Auswirkungen und Massnahmen dokumentiert und die Dokumentation mindestens zwei Jahre aufbewahrt wird **Art. 15 DSV**. Im Crawler-Fall bestätigte das Bundesverwaltungsgericht die Anordnung des EDÖB, die Betroffenen zu informieren. Wo die Einzelinformation unmöglich oder unverhältnismässig ist, darf eine öffentliche Bekanntmachung an ihre Stelle treten **a-3790-2024**.

Aufsichtsrechtliche Durchsetzung durch den EDÖB

Der EDÖB eröffnet eine Untersuchung, wenn genügend Anzeichen für einen Verstoß bestehen. Bei geringfügiger Bedeutung kann er davon absehen (Art. 49 Abs. 1 und 2 DSG) **Art. 49 DSG**. Kommt der Betroffene seinen Mitwirkungspflichten nicht nach, kann der EDÖB unter anderem Zugang zu Räumlichkeiten und Anlagen sowie Begutachtungen durch Sachverständige anordnen (Art. 50 DSG) **Art. 50 DSG**. Er kann insbesondere verfügen, dass die Vorkehrungen nach Art. 7 und 8 DSG getroffen werden (Art. 51 Abs. 3 lit. b DSG).

Stellt der Betroffene die Einhaltung während der Untersuchung selbst wieder her, kann der EDÖB sich auf eine Verwarnung beschränken (Abs. 5) **Art. 51 DSG**. Die vorsätzliche Missachtung einer Verfügung, die unter Hinweis auf die Strafdrohung ergangen ist, ist für private Personen strafbar (Art. 63 DSG) **Art. 63 DSG**. Unter altem Recht konnte der EDÖB im Klageverfahren keine technischen und organisatorischen Massnahmen verlangen, die über seine Empfehlung hinausgingen **a-5225-2015**. Diese Schranke ist mit der Verfügungsbefugnis nach Art. 51 DSG weitgehend überholt.

Wer Anzeige erstattet, hat keinen Anspruch auf eine Untersuchung. Das Bundesverwaltungsgericht stellte fest: «la personne concernée ne bénéficie pas d'un droit subjectif à ce qu'une procédure d'enquête soit ouverte» (die betroffene Person hat kein subjektives Recht auf die Eröffnung einer Untersuchung). Die Mitteilung nach Art. 49 Abs. 4 DSG ist keine anfechtbare Verfügung **a-8391-2025**. Betroffene müssen ihre Rechte deshalb auf dem Zivilweg durchsetzen (unten).

Strafrechtliche Folgen: Art. 61 lit. c DSG

Mit Busse bis 250 000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich die Mindestanforderungen an die Datensicherheit nicht einhalten, die der Bundesrat nach Art. 8 Abs. 3 DSG erlassen hat **Art. 61 DSG**. Daraus ergeben sich drei Schranken. Bundesorgane sind nicht erfasst. Fahrlässigkeit ist straflos, wie der Erläuternde Bericht zur DSV bestätigt.

EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) -

. Und die Tat wird nur auf Antrag verfolgt. Verfolgung und Beurteilung obliegen den Kantonen; der EDÖB kann Anzeige erstatten und die Rechte einer Privatküglerschaft wahrnehmen **Art. 65 DSG**. In Geschäftsbetrieben gelten Art. 6 und 7 VStrR. Bei Bussen bis 50 000 Franken kann anstelle der verantwortlichen Personen der Betrieb verurteilt werden, wenn deren Ermittlung unverhältnismässig wäre **Art. 64 DSG**. Die Verfolgung verjährt nach fünf Jahren **Art. 66 DSG**.

Der Tatbestand war im Parlament umstritten. Der Nationalrat strich die Strafnorm (Art. 55 Bst. c E-DSG) zunächst **AB 2019 N 1805**. In der Differenzvereinbarung beantragte eine Minderheit erneut die Streichung wegen Unbestimmtheit. Der Bundesrat entgegnete: «Der Bundesrat ist also in der Festlegung der Mindestanforderungen nicht einfach frei.» Der Nationalrat folgte mit 137 zu 51 Stimmen der Mehrheit, und die Strafnorm blieb bestehen **AB 2020 N 140**. Die Spannung zwischen einer Blankettstrafnorm und einem offenen, risikobasierten Ordnungsmassstab löst die kantonale Praxis über eine enge Auslegung. Die Genfer Chambre pénale de recours hält fest: «seuls des cas manifestes - par exemple l'absence totale de mesures de protection - pourraient constituer une infraction pénale» (nur offenkundige Fälle, etwa das völlige Fehlen von Schutzmassnahmen, eine Straftat darstellen) **ACPR/239/2025**. Das Obergericht Zürich bestätigte eine Nichtanhandnahme, weil bei TLS-verschlüsseltem Versand kein vorsätzlicher Verstoß ersichtlich war **UE240472**. Die Waadtländer Chambre des recours pénale sah im Versand von Briefen an eine falsche Adresse durch ein Spital höchstens eine nicht strafbare Fahrlässigkeit; die Frage der Datensicherheit liess sie offen **CREP pe22-008518-471/2023**. Diese kantonalen Entscheide folgen einer übereinstimmenden Linie, binden aber nicht über den jeweiligen Kanton hinaus.

Zivilrechtliche Folgen und Haftung

Für private Bearbeiter liegt eine Persönlichkeitsverletzung insbesondere vor, wenn Personendaten entgegen den Grundsätzen nach Art. 6 und 8 DSG bearbeitet werden (Art. 30 Abs. 2 lit. a DSG) **Art. 30 DSG**. Die Datensicherheit ist damit ausdrücklich ein Bearbeitungsgrundsatz, dessen Missachtung die Persönlichkeit verletzt. Widerrechtlich ist die Verletzung, wenn sie nicht durch Einwilligung, ein überwiegendes Interesse oder Gesetz gerechtfertigt ist (Art. 31 Abs. 1 DSG) **Art. 31 DSG**. Die Klagen richten sich nach Art. 28, 28a und 28g bis 28l ZGB. Verlangt werden können namentlich das Verbot einer Bearbeitung, die Untersagung einer Bekanntgabe

sowie Löschung oder Vernichtung, ferner die Mitteilung oder Veröffentlichung des Urteils (Art. 32 Abs. 2 und 4 DSG) **Art. 32 DSG**. Für Schadenersatz und Genugtuung gelten über den Verweis in Art. 32 Abs. 2 DSG die Regeln des ZGB.

Bei Schadenersatzklagen ist der Kausalzusammenhang häufig das entscheidende Hindernis. Das Verwaltungsgericht Glarus bejahte die Widerrechtlichkeit einer teilweise unzulässigen Datenweitergabe durch das Strassenverkehrsamt, wies das Staatshaftungsbegehren aber ab: «Damit mangelt es diesbezüglich an der erforderlichen Kausalität.» **VG.2016.00090**. Der Fall betraf eine unzulässige Bekanntgabe nach kantonalem Staatshaftungsrecht, nicht ein Versagen der Sicherheitsmassnahmen nach Art. 32 DSG. Er zeigt aber, dass die Feststellung eines Datenschutzverstosses allein keinen Ersatzanspruch begründet.

Hinweise für die Praxis

- Schutzbedarf und Risiko nach Art. 1 DSV schriftlich beurteilen und die gewählten Massnahmen begründen, insbesondere wo der Stand der Technik oder Kosten eine Rolle spielen. Diese Dokumentation belegt im Aufsichtsverfahren und gegenüber einem Strafvorwurf, dass Massnahmen risikobasiert gewählt wurden.
- Zugriffsrechte am Bedarf ausrichten, Ausnahmezugriffe begründen lassen und protokollieren, Protokolle nur zweckgebunden verwenden.
- Auftragsbearbeiter vertraglich auf Sicherheitsmassnahmen, Datenlebenszyklus, Audits und Unterauftragsgenehmigung verpflichten, weil Art. 61 lit. b DSG die vorsätzliche Übergabe ohne Vergewisserung unter Strafe stellt.
- Bei Bundesorganen die Übergangsfristen von Art. 46 DSV für Prüfung und Implementierung der Protokollierung überwachen (oben, Protokollierung).
- Nach einem Vorfall Verletzungen nach Art. 15 Abs. 4 DSV dokumentieren und die Meldeschwelle des hohen Risikos prüfen; nachträgliche Sperren ersetzen diese Prüfung nicht (oben, Verletzung der Datensicherheit).