Kommentar zu Art. 5 DSG: Begriffe

Funktion des Begriffskatalogs und Systemwechsel von 2020

Art. 5 DSG enthält die Legaldefinitionen, an die das gesamte Gesetz anknüpft. Die Begriffe entscheiden darüber, ob das DSG überhaupt anwendbar ist (Personendaten natürlicher Personen, bearbeitet durch private Personen oder Bundesorgane, Art. 2 Abs. 1 DSG **Art. 2 DSG**). Sie lösen zudem qualifizierte Rechtsfolgen aus, namentlich nach Art. 6 Abs. 7, Art. 22, Art. 24, Art. 30 und Art. 34 DSG; diese werden bei den jeweiligen Begriffen behandelt (besonders schützenswerte Personendaten, Profiling, Verletzung der Datensicherheit). Die Qualifikation nach Art. 5 ist deshalb häufig ergebnisbestimmend.

Art. 5 DSG ist seit dem Inkrafttreten am 1. September 2023 unverändert; spätere Änderungen des Gesetzes betreffen andere Bestimmungen, namentlich Art. 24 Abs. 5bis DSG **Art. 24 DSG**.

Die Totalrevision hat den Katalog gegenüber Art. 3 aDSG umgebaut. Die Botschaft nennt als Leitlinie die Modernisierung der Terminologie, "insbesondere um die Vereinbarkeit mit dem Recht der Europäischen Union zu verbessern" **BBl 2017 6941**. Im Einzelnen:

- Der Schutz von Daten juristischer Personen entfällt; er sei "nur von geringer praktischer Bedeutung" gewesen **BBl 2017 6941**.
- Der Begriff der Datensammlung entfällt, weil Daten "heute wie eine Datensammlung genutzt werden, auch wenn sie nicht zentral gespeichert sind" **BBl 2017 6941**.
- Das Persönlichkeitsprofil, eine schweizerische Besonderheit, wird durch das Profiling abgelöst; der "Inhaber der Datensammlung" durch den "Verantwortlichen" **BBl 2017 6941**.
- Genetische und biometrische Daten werden besonders schützenswert; die Verletzung der Datensicherheit und der Auftragsbearbeiter werden neu definiert **BBl 2017 6941**.
- Das Profiling mit hohem Risiko (lit. g) fehlte im Entwurf und ist ein parlamentarischer Kompromiss (unten, Profiling).

Die Angleichung an das EU-Recht ist nach der Botschaft eine Annäherung an die Verordnung (EU) 2016/679, keine Übernahme **BBl 2017 6941**. Für den Verantwortlichen und den Auftragsbearbeiter verweist die Botschaft ausdrücklich auf die entsprechenden Begriffe der DSGVO und des revidierten Übereinkommens SEV 108 **BBl 2017 6941**. Die europäischen Begriffe sind damit ein Auslegungsgesichtspunkt; sie verdrängen den schweizerischen Wortlaut aber nicht, wie gerade lit. g zeigt. Bei der Datensicherheit hat das Obergericht Zürich die DSGVO als Massstab herangezogen und festgehalten, dass Unternehmen, welche die technischen und organisatorischen Anforderungen der DSGVO erfüllen, auch dem schweizerischen Recht genügen **UE240472**.

Für die Fortgeltung der Rechtsprechung zum alten Recht ist zu differenzieren. Das Bundesgericht wendet Art. 5 lit. a DSG mit der bisherigen Formel an und hält, bezogen auf das Auskunftsrecht, fest, dass die Rechtsprechung zum aDSG "reste en principe valable" (grundsätzlich gültig bleibt) **4A_504/2025**. Wo der Wortlaut übernommen wurde (Personendaten, Bearbeiten, Bekanntgeben, Bundesorgan), dienen ältere Entscheide weiterhin als Auslegungshilfe; wo der Begriff neu gefasst wurde (Profiling, Verantwortlicher, genetische und biometrische Daten), ist die Übertragung gesondert zu begründen.

Personendaten (lit. a)

Angaben mit Personenbezug

Personendaten sind "alle Angaben", die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Der Begriff ist medienneutral: Auch Bilder sind Personendaten, "ohne dass es auf die Beschaffenheit des Datenträgers ankommt" **BGE 138 II 346**. Erfasst sind Tatsachen und Werturteile. Personendaten können nach dem Bundesgericht "consister en des constatations de fait ou en des jugements de valeur se rapportant à la personne en cause" (aus Tatsachenfeststellungen oder aus Werturteilen über die betreffende Person bestehen) **4A_504/2025**. Im entschiedenen Fall waren Aussagen in einem internen Untersuchungsbericht über das Verhalten eines Professors zugleich Daten des Professors und der befragten Personen; Passagen, die nur Zweck, Chronologie der Untersuchung oder Dritte betrafen, waren keine Personendaten des Gesuchstellers **4A_504/2025**. Der Personenbezug ist also passagenweise zu prüfen, und dieselbe Angabe kann mehreren betroffenen Personen zugeordnet sein.

Einen Personenbezug verneint hat das Genfer Obergericht bei einer bloss funktionalen Erwähnung: Die Nennung des Geschäftsführers als Vertreter der Gesellschaft in Kontrollberichten enthielt keine Information über seine persönliche Situation; die Daten betrafen die Gesellschaft selbst, die durch ihre Organe handelt **ACJC/1571/2025**. Diese kantonale Anwendung verhindert, dass der Ausschluss juristischer Personen über deren Organe umgangen wird.

Bestimmbarkeit nach dem relativen Ansatz

Bestimmbar ist eine Person, wenn auf sie aufgrund zusätzlicher Informationen geschlossen werden kann; "jede theoretische Möglichkeit der Identifizierung" genügt nicht **BGE 136 II 508**. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung kein Interessent ihn auf sich nehmen wird, fehlt die Bestimmbarkeit **BGE 136 II 508**. Massgebend sind der objektiv erforderliche Aufwand und das Interesse des Datenbearbeiters oder eines Dritten an der Identifizierung **BGE 136 II 508**.

Die Beurteilung erfolgt "aus der Sicht des jeweiligen Inhabers der Information"; bei einer Weitergabe genügt es, "wenn der Empfänger die betroffene Person zu identifizieren vermag" **BGE 136 II 508**. Im Logistep-Fall waren deshalb auch dynamische IP-Adressen Personendaten, weil das Geschäftsmodell auf der späteren Identifizierung der Anschlussinhaber durch die Rechteinhaber beruhte; es genügte, dass die Bestimmbarkeit für einen Teil der gespeicherten Informationen gegeben war **BGE 136 II 508**. Das Fernmeldegesetz stand der Anwendung des DSG nicht entgegen **BGE 136 II 508**.

Die weitere Rechtsprechung zeigt die Bandbreite:

- Eindeutige Identifikatoren. In einem archivierten Stichprobenrahmen des BFS blieben die Angaben Personendaten, weil das BFS sie über die AHV-Nummer mit dem Adressverzeichnis verknüpfen konnte; die Archivierung änderte daran nichts **1C_425/2020**.
- Pseudonymisierung. Sie beseitigt den Personenbezug nicht, wenn der Empfänger die Person aus Daten und Kontext

bestimmen kann. Bei der Übermittlung von Mitarbeiter- und Kontodaten an das US-Justizdepartement genügten die Leaver-Liste und das Factsheet mit dem Namen des Kundenberaters; ob das Zusatzwissen der US-Behörden über SWIFT-Daten hinzukam, liess das Bundesgericht offen **4A_365/2017**.
- Bilder. Bei Street View genügten Gesichter, Fahrzeugkennzeichen sowie Abbildungen von Häusern, Gärten und Höfen, weil sich ein Personenbezug problemlos herstellen lässt **BGE 138 II 346**.
- Wirksame Anonymisierung. Anonymisierte Rechnungen und medizinische Unterlagen enthalten keine Personendaten im Sinne von Art. 5 lit. a DSG, wenn sie keine Angaben enthalten, die auf eine bestimmte versicherte Person schliessen lassen; die Schutzbestimmungen für Gesundheitsdaten sind dann gegenstandslos **BGE 151 V 30**. Nach der Botschaft gilt das Gesetz nicht für anonymisierte Daten, wenn eine Reidentifizierung durch Dritte unmöglich ist **BBl 2017 6941**.

Die Entscheide zum Stichprobenrahmen **1C_425/2020** und zu den anonymisierten Rechnungen **BGE 151 V 30** widersprechen sich nicht: Entscheidend ist jeweils, ob beim konkreten Inhaber oder Empfänger ein realistisch nutzbares Zuordnungsmerkmal vorhanden ist. Wer sich auf Anonymisierung beruft, muss deshalb darlegen, dass weder er noch der Empfänger über einen solchen Schlüssel verfügt.

Betroffene Person (lit. b)

Ausschluss juristischer Personen und Übergang

Betroffene Person ist nur die natürliche Person, über die Personendaten bearbeitet werden. Die Botschaft verweist juristische Personen auf andere Schutzinstrumente, namentlich den Schutz der Privatsphäre nach Art. 13 BV, den Persönlichkeitsschutz des ZGB und das UWG **BBl 2017 6941**.

Die Gerichte wenden den Ausschluss konsequent an. Nach dem Bundesverwaltungsgericht hat das neue DSG den Datenschutz juristischer Personen aufgehoben; Auskunftsbegehren nach DSG können nur noch die Daten der beteiligten natürlichen Person betreffen **a-1251-2024**. Das Genfer Obergericht wendete das revidierte DSG sofort auf einen hängigen Zivilprozess an; die klagende Gesellschaft verlor ihre Aktivlegitimation während des Verfahrens **ACJC/1571/2025**. Für Rechtsmittelverfahren hält das Bundesverwaltungsgericht unter Hinweis auf Art. 70 DSG fest, dass das neue Recht auf hängige Beschwerden gegen erstinstanzliche Entscheide anwendbar ist, die nach dem Inkrafttreten ergangen sind **a-1251-2024**.

Eine befristete Übergangsregel besteht nur für Bundesorgane: Vorschriften anderer Bundeserlasse über Personendaten gelten während fünf Jahren nach Inkrafttreten weiter für Daten juristischer Personen, insbesondere für Bekanntgaben nach Art. 57s Abs. 1 und 2 RVOG **Art. 71 DSG**. Die Botschaft begründet dies mit der Vermeidung von Rechtslücken **BBl 2017 6941**. Für private Verantwortliche sieht Art. 71 DSG keine entsprechende Frist vor **Art. 71 DSG**.

Daten Verstorbener

Das DSG regelt die Daten Verstorbener nicht ausdrücklich. Das Verwaltungsgericht Bern hat zum kantonalen Datenschutzrecht entschieden, dass der Persönlichkeitsschutz mit dem Tod endet und "Informationen über Verstorbene" deshalb keine Personendaten sind; Angehörige können sich aber auf ihr eigenes Persönlichkeitsrecht berufen, wenn es um den Andenkensschutz geht oder die Informationen sich zugleich auf lebende Personen beziehen, etwa bei Erbkrankheiten **100 2023 151**. Der Entscheid betrifft kantonales Recht; seine Begründung knüpft aber an die natürliche Person an und passt zu lit. a und b DSG.

Kantonales Recht kann abweichen. Das Genfer Recht (LIPAD) behandelt Daten Verstorbener als Personendaten mit eigenem Zugangsregime, das ein schutzwürdiges Interesse der Angehörigen und eine Abwägung mit dem bekannten oder mutmasslichen Willen der verstorbenen Person verlangt; es erfasst zudem juristische Personen des Privatrechts **ATA/229/2018**. Zum alten Bundesrecht entschied das Bundesgericht, dass der datenschutzrechtliche Auskunftsanspruch nicht auf die Erben übergeht; ob die Verordnungsbestimmung über die Auskunft an nahe Verwandte Verstorbener gesetzmässig war, liess es offen **BGE 140 V 464**. Angehörige sind daher regelmässig auf spezialgesetzliche Einsichtsrechte oder ihr eigenes Persönlichkeitsrecht verwiesen.

Besonders schützenswerte Personendaten (lit. c)

Abschliessender Katalog und formale Qualifikation

Der Katalog von lit. c ist abschliessend. Das Genfer Strafbeschwerdegericht hält zum geltenden Recht fest, die sensiblen Informationen seien "énumérées, de façon exhaustive, à l'art. 5 let. c" (in Art. 5 lit. c abschliessend aufgezählt) **ACPR/892/2024**; das Bundesgericht hatte dies bereits für Art. 3 lit. c aDSG so gesehen und daraus abgeleitet, dass Angaben über Einkommen und Vermögen nicht dazu gehören **1P.79/2000**. Ebenso wenig sind eine Lieferadresse, gekaufte Gegenstände und der Kaufpreis besonders schützenswert, auch wenn die Gefahr gerade aus der Verwendung des Datums in einem bestimmten Kontext folgt **SBE.2022.45/46**. Finanz- und Adressdaten rechtfertigen nach dem Obergericht Zürich auch keinen erhöhten Sicherheitsstandard wie eine Ende-zu-Ende-Verschlüsselung **UE240472**.

Die Qualifikation ist nach der Waadtländer Rechtsprechung abstrakt: Es genüge, dass ein Datum eines der aufgezählten Themen betrifft, unabhängig vom tatsächlichen Verletzungspotenzial **CREP pe23-017055-51/2024**. Das schliesst nicht aus, Daten einzubeziehen, die mittelbare Rückschlüsse erlauben. Die Abgrenzung erfolgt beim Inhalt der Angabe: Erst wenn diese tatsächlich etwas über die geschützte Kategorie aussagt, liegt ein besonders schützenswertes Datum vor.

Die Rechtsfolgen sind erheblich: ausdrückliche Einwilligung nach Art. 6 Abs. 7 lit. a DSG **Art. 6 DSG**, Regelvermutung der Persönlichkeitsverletzung bei Bekanntgabe an Dritte nach Art. 30 Abs. 2 lit. c DSG, vorbehältlich allgemein zugänglich gemachter Daten nach Abs. 3 **Art. 30 DSG**, Gesetz im formellen Sinn für Bundesorgane nach Art. 34 Abs. 2 lit. a DSG, mit den Erleichterungen von Abs. 3 und 4 **Art. 34 DSG**. Ein hohes Risiko, das eine Datenschutz-Folgenabschätzung auslöst, nimmt Art. 22 Abs. 2 lit. a DSG namentlich bei der umfangreichen Bearbeitung solcher Daten an; die Sensibilität allein genügt nach dem Wortlaut nicht **Art. 22 DSG**.

Ansichten und Tätigkeiten (Ziff. 1)

Das Bundesverwaltungsgericht hat Ziff. 1 im Fall "Pfarrer-Check" angewendet: Eine öffentlich einsehbare Datenbank, die Pfarrpersonen mit dem Status "erfasst" oder "angefragt" zu einem Fragebogen über ihre religiösen Ansichten verzeichnete, bearbeitete besonders schützenswerte Daten; die Verletzung von Verhältnismässigkeit, Zweckbindung und Transparenz stellte eine Persönlichkeitsverletzung nach Art. 30 Abs. 2 lit. a und c DSG dar, ohne Rechtfertigungsgrund **a-2941-2024**. Bereits der Status erlaubte also einen Rückschluss auf die religiöse Haltung.

Mittelbare Angaben genügen, wenn sie die Haltung offenlegen. Das Bundesgericht qualifizierte die Mitgliedschaft in einem Verein als besonders schützenswert, weil sie "eine bestimmte weltanschauliche sowie politische Haltung zum Ausdruck" bringt; ihre systematische Erfassung durch eine kantonale Verwaltung verlangte eine klare gesetzliche Grundlage **BGE 122 I 360**. Umgekehrt sind nicht alle Angaben in einem religiös geprägten Dokument sensibel: Nach dem Genfer Verfassungsgericht waren nicht die Namen der Beschwerdeführerinnen, sondern deren geschilderte religiöse Erfahrung besonders schützenswert; das Genfer Recht erfasst zudem

kulturelle Ansichten und ist insoweit weiter als lit. c Ziff. 1 **ACST/21/2019**.

Gesundheit, Intimsphäre, Rasse und Ethnie (Ziff. 2)

Gesundheitsdaten sind solche, die direkt oder indirekt Schlüsse auf den physischen, geistigen oder psychischen Zustand einer Person zulassen **ACPR/892/2024**. Rein administrative Daten einer Klinik erfüllen diese Voraussetzung nicht **ACPR/892/2024**. Die Schwelle zeigt sich bei generischen Krankheitshinweisen: Der Vermerk "malattia" als Abwesenheitsgrund in einem Dienstplan sagt nach dem Tessiner Gericht nichts über Zustand, Art oder Schwere der Krankheit aus und ist kein besonders schützenswertes Datum **60.2018.232**. Ähnlich bezweifelte das Neuenburger Kantonsgericht, dass der blosse Hinweis auf "problèmes de santé" sensibel sei, hielt aber fest, anders wäre zu entscheiden, wenn Einzelheiten zur Art der Probleme bekanntgegeben worden wären **CCP.2010.17**. Diese Entscheide betreffen Strafbestimmungen und das alte Recht; sie zeigen aber eine übereinstimmende Linie: Massgebend ist der Informationsgehalt über den Gesundheitszustand, nicht das Stichwort.

Zur Intimsphäre hat das Appellationsgericht Basel-Stadt nach kantonalem Recht entschieden, dass Abklärungen wegen sexueller Belästigung die Geheimsphäre der beschuldigten Personen und der mutmasslichen Opfer direkt betreffen; der sensible Charakter schloss den Zugang aber nicht per se aus, sondern führte zu Interessenabwägung und Anonymisierung **VD.2021.148**.

Genetische und biometrische Daten (Ziff. 3 und 4)

Der unterschiedliche Wortlaut von Ziff. 3 und 4 ist gewollt. Der Nationalrat wollte nur genetische Daten erfassen, die eine Person eindeutig identifizieren **AB 2020 N 140**. Der Ständerat hielt an der weiten Fassung fest, mit der Begründung: "Genetische Daten sind immer besonders schützenswerte Personendaten, auch wenn sie nicht zur Identifikation einer Person führen." **AB 2020 S 291** Das Gesetz enthält die Identifikationsschranke deshalb nur bei den biometrischen Daten.

Biometrische Daten sind nach der Botschaft Personendaten, die durch ein spezifisches technisches Verfahren zu physischen, physiologischen oder verhaltenstypischen Merkmalen gewonnen werden und die eindeutige Identifizierung ermöglichen oder bestätigen **BBl 2017 6941**. Das Bundesgericht hat Daten aus automatisierter Gesichtserkennung als besonders schutzwürdige Daten im Sinne von Art. 5 lit. c Ziff. 4 DSG eingeordnet und auf das Risiko falsch-positiver Ergebnisse bei grossen Personenkreisen hingewiesen **BGE 151 I 137**. Unter altem Recht hielt das Bundesverwaltungsgericht fest, Fingerabdrücke und die daraus extrahierten Minutien seien einer bestimmten Person zuzuordnen, unabhängig von der Speicherform als Template; die zentrale Speicherung verletzte die Verhältnismässigkeit **2009-44**.

Für DNA-Profile aus nicht codierenden Abschnitten hat das Bundesgericht unter Art. 13 Abs. 2 BV entschieden, dass sie, ähnlich einem Fingerabdruck, nur persönlichkeitsneutrale Identifikationsmerkmale enthalten und ihre Erstellung und Speicherung leichte Eingriffe sind **BGE 128 II 259**. Dieser Entscheid betrifft die Schwere des Grundrechtseingriffs, nicht die Kategorie nach Art. 5 lit. c; er steht der gesetzgeberischen Entscheidung, genetische Daten stets als besonders schützenswert zu behandeln, nicht entgegen, kann aber bei der Verhältnismässigkeit einer Bearbeitung weiterhin Gewicht haben. Die Waadtländer Praxis zeigt, dass biometrische Daten (AFIS) und DNA-Profile (CODIS) getrennt geführt und nur über eine Prozesskontrollnummer verknüpft werden, damit die DNA-Profile anonym bleiben **CREP 397/2026**.

Verfolgungen und Sanktionen (Ziff. 5)

Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen sind besonders schützenswert. Die frühere Eidgenössische Datenschutzkommission folgerte daraus, dass ein Bundesorgan einer anderen Behörde nur bekanntgeben darf, was diese im Einzelfall für ihre gesetzliche Aufgabe benötigt; die Herausgabe eines ganzen Strafdossiers samt gelöschter Strafregistereinträge war unzulässig, wo die Beantwortung zweier Fragen genügt hätte **150003905**. Das Bundesgericht behandelte die Information über eine Verwaltungssanktion (Ausschluss von öffentlichen Beschaffungen) in analoger Anwendung des alten Rechts als sensibles Datum und erklärte die automatische Publikation im Amtsblatt als unverhältnismässig, die befristete Publikation auf der Website der Aufsichtsbehörde dagegen als zulässig **BGE 148 I 226**. Die Kategorie reicht damit über das Strafverfahren hinaus.

Die Grenze liegt beim Bezug zu einer Verfolgung oder Sanktion. Ein Polizeijournal, das Aussagen bei einem Einsatz im Konditional zusammenfasst und keine Verfolgung oder Sanktion erwähnt, enthielt nach dem Genfer Verwaltungsgericht keine sensiblen Daten **ATA/1254/2024**. Werden Gerichtsakten wissenschaftlich ausgewertet, verlangte das Obergericht Schaffhausen nach kantonalem Recht, dass Täter und Opfer in der Publikation nicht bestimmbar sind **Nr. 95/2001/3**.

Massnahmen der sozialen Hilfe (Ziff. 6)

Die Reichweite der Kategorie zeigt sich namentlich in der kantonalen Praxis zu gleichlautenden Bestimmungen. Das Genfer Verwaltungsgericht qualifizierte Informationen über die Sozialhilfe einschliesslich der Weigerung zur Mitwirkung und der Einstellung der Leistungen als sensibel und erklärte ihre nicht erforderliche Weitergabe an die Ergänzungsleistungsstelle für widerrechtlich **ATA/3/2026**. Das Bundesgericht bestätigte unter Willkürkognition, dass ein Kindesschutzdossier sensible Daten über Gesundheit, Intimsphäre und Hilfsmassnahmen des Kindes enthält, und liess deshalb die Verweigerung der Einsicht durch die Pflegeeltern zu **1C_376/2022**. Nach dem Obergericht Bern fällt dagegen das Gesuch um unentgeltliche Rechtspflege nicht unter die soziale Hilfe, weil es auf dem Prozessrecht und nicht auf dem Sozialhilferecht beruht **BK 2018 240**. Der Datenschutzbeauftragte des Bundes ordnete 1997 auch Arbeitslosendaten der sozialen Hilfe zu **150003584**; diese weite Verwaltungsauffassung zum alten Recht ist mit Zurückhaltung heranzuziehen.

Bearbeiten und Bekanntgeben (lit. d und e)

Weiter Bearbeitungsbegriff

Bearbeiten ist "jeder Umgang" mit Personendaten, unabhängig von Mitteln und Verfahren. Nach der Botschaft bleibt der Begriff inhaltlich unverändert; die Aufzählung wurde um Speichern und Löschen ergänzt **BBl 2017 6941**. Bereits das Erstellen von Aufnahmen im öffentlichen Raum, auf denen Personen oder Autokennzeichen erkennbar sind, ist Bearbeiten; das Bundesgericht qualifizierte Dashcam-Aufnahmen zudem als für andere Verkehrsteilnehmer nicht erkennbar und damit als heimlich, was zur Rechtswidrigkeit der Aufzeichnung führte **BGE 146 IV 226**. Die Veröffentlichung von Bildern im Internet ist ebenfalls Bearbeiten **BGE 138 II 346**.

Bekanntgeben: Übermitteln oder Zugänglichmachen

Bekanntgeben umfasst das aktive Übermitteln und das passive Zugänglichmachen. Das Bundesverwaltungsgericht hat unter geltendem Recht entschieden, dass das Publizieren von Schuldnerdaten auf einer Internetseite Bekanntgeben im Sinne von Art. 5 lit. e DSG und damit Bearbeiten ist; die Publikation verletzte die Verhältnismässigkeit und war nicht gerechtfertigt **a-3891-2025**. Im Moneyhouse-Entscheid erstreckte das Gericht die Bekanntgabe auf Verlinkungen, die Premium-Usern die Verknüpfung privater Informationen zu Wohnsituation, Nachbarn und Haushaltsmitgliedern ermöglichten; dass die Seiten suchmaschinenindexiert waren und Betroffene nachträglich die Löschung verlangen konnten, ersetzte die Einwilligung nicht **a-4232-2015**.

Bekanntgabe setzt einen Empfänger voraus, der die Daten nicht bereits kennt. Das Bundesverwaltungsgericht verneinte eine Bekanntgabe, als ein Militärversicherer einer Stelle lediglich mitteilte, zwei von ihr gemeldete Medikamente würden nicht vergütet; die Stelle besass diese Informationen bereits, anders wäre es bei Angaben über die versicherte Krankheit gewesen **a-7372-2006**. Dritte sind nach dem Pensionskassenentscheid all jene, welche die Daten für ihre Aufgabe nicht benötigen: Der offene Versand von Vorsorgeausweisen an die Arbeitgebenden war eine Bekanntgabe, soweit die Ausweise Daten enthielten, die diese nicht schon aus ihrer Beitragspflicht kannten **2012-14**.

Rechtliche Selbständigkeit innerhalb eines Konzerns schliesst die Bekanntgabe nicht aus. Beschaffte die Zusatzversicherung des Helsana-Konzerns Daten bei den konzerneigenen Grundversicherern, war dies "gleichzeitig eine Bekanntgabe von Daten" durch diese, die mangels gültiger schriftlicher Einwilligung im Einzelfall unrechtmässig war **a-3548-2018**. Kantonal entschied das Verwaltungsgericht Zürich, dass die Weitergabe von Adressen durch einen städtischen Netzbetreiber an private Telekommunikationsanbieter eine Bekanntgabe ohne gesetzliche Grundlage und keine Auslagerung war, weil die Anbieter eigene Geschäftszwecke verfolgten **VB.2020.00700**.

Profiling und Profiling mit hohem Risiko (lit. f und g)

Profiling als automatisierte Bewertung

Profiling setzt eine automatisierte Bearbeitung voraus, die persönliche Aspekte einer natürlichen Person bewertet. Die Botschaft betont, der Begriff sei an die europäische Terminologie angepasst und erfasse "nur noch die automatisierte Bearbeitung von Personendaten" **BBl 2017 6941**. Manuelle Zusammenstellungen fallen daher nicht unter lit. f, auch wenn sie unter dem alten Recht ein Persönlichkeitsprofil sein konnten.

Das Bundesgericht hat die polizeiliche Erstellung von Bewegungsprofilen aus automatischer Fahrzeugfahndung als "Anwendungsfall des datenschutzrechtlich besonders heiklen" Profilings bezeichnet und auf die kaum nachvollziehbare Entscheidfindung komplexer algorithmischer Systeme hingewiesen **BGE 151 I 137**; der Entscheid beruht auf kantonalem Polizeirecht und Art. 13 BV, nicht unmittelbar auf lit. f. Am anderen Ende stehen Einzelaufnahmen: Fotos einer Person beim Entsorgen von Abfall hielten nach der Waadtländer Rechtsprechung "un instant isolé de vie" (einen isolierten Lebensmoment) fest und dienten nicht der Erstellung eines Profils **CREP pe23-017055-51/2024**.

Für Private hat das einfache Profiling keine besonderen Rechtsfolgen; für Bundesorgane verlangt es eine ausdrückliche Einwilligung, soweit diese die Grundlage bildet, und ein Gesetz im formellen Sinn (Art. 6 Abs. 7 lit. c DSG **Art. 6 DSG**; Art. 34 Abs. 2 lit. b DSG **Art. 34 DSG**).

Profiling mit hohem Risiko als parlamentarischer Kompromiss

Lit. g ist das Ergebnis der längsten Differenz der Revision. Der Nationalrat hielt die Kategorie für einen "Swiss Finish", weil die DSGVO keine solche Unterscheidung kenne **AB 2020 N 140**, und strich die Bestimmung in der Differenzbereinigung mit 98 zu 88 Stimmen **AB 2020 N 1598**. Der Ständerat richtete die Definition bewusst an "der Definition des Persönlichkeitsprofils im geltenden Recht" aus **AB 2020 S 291**; der Bundesrat erklärte, damit lasse sich "ein vergleichbares Schutzniveau wie heute mit den Vorschriften zum Persönlichkeitsprofil" erreichen **AB 2020 N 140**. Die Einigungskonferenz folgte dem Ständerat nach der Zusicherung, die Fassung bringe "ni une complication des procédures ni une augmentation de la protection" (weder eine Verkomplizierung der Verfahren noch eine Erhöhung des Schutzes) gegenüber dem bisherigen Recht und der Moneyhouse-Rechtsprechung **AB 2020 N 1817**.

Diese Materialien sind für die Auslegung bedeutsam: Sie sprechen dafür, lit. g am Massstab des früheren Persönlichkeitsprofils und namentlich des Moneyhouse-Entscheids zu messen. Dort genügte die systematische Verknüpfung auch öffentlich zugänglicher oder nicht besonders schützenswerter Daten, wenn sie "Aufschluss über einen oder mehrere wesentliche Aspekte der Persönlichkeit" gab, etwa über die private Wohn- und Lebenssituation **a-4232-2015**. Auch die Verfeinerung von Adressprofilen durch Spendenverhalten galt der Verwaltungspraxis als Persönlichkeitsprofil **150001706**. Keine Beurteilung wesentlicher Persönlichkeitsaspekte erlaubte dagegen eine einzelne Rechnungskopie mit Lieferadresse und gekauften Gegenständen **SBE.2022.45/46**. Anders als das Persönlichkeitsprofil setzt lit. g aber ein Profiling und damit Automatisierung voraus; zudem muss das hohe Risiko für Persönlichkeit oder Grundrechte gerade aus der Verknüpfung folgen.

Eine Variante, die das hohe Risiko an die Herleitung besonders schützenswerter Daten knüpfen wollte, lehnte der Bundesrat ab, weil in diesem Fall ohnehin die qualifizierten Rechtsfolgen für solche Daten gelten **AB 2020 N 140**. Rechtsfolge des Profilings mit hohem Risiko durch Private ist die ausdrückliche Einwilligung, soweit eine Einwilligung erforderlich ist (Art. 6 Abs. 7 lit. b DSG **Art. 6 DSG**). Zu Bonitätsbewertungen prüfte das Obergericht Bern eine negative Bonitätsauskunft allein am Rechtfertigungsgrund der Kreditwürdigkeitsprüfung, ohne sie als Profiling einzuordnen **BK 2024 170**.

Verletzung der Datensicherheit (lit. h)

Eine Verletzung der Datensicherheit liegt vor, wenn Personendaten verlorengehen, gelöscht, vernichtet oder verändert oder Unbefugten offengelegt oder zugänglich gemacht werden. Nach der Botschaft gilt dies "ungeachtet davon, ob der Vorgang mit Absicht geschieht oder nicht, ob er widerrechtlich ist oder nicht" **BBl 2017 6941**. Der Begriff ist erfolgsbezogen: Er beschreibt das Ergebnis, nicht eine Pflichtverletzung.

Das Bundesverwaltungsgericht lässt bereits die blosse Möglichkeit genügen, dass Unbefugte auf die Daten zugreifen können; ob ein tatsächlicher Zugriff stattfand, ist irrelevant. Im entschiedenen Fall waren URLs mit Personendaten von einer Suchmaschine indexiert worden **a-3790-2024**. Ebenso fehlte die Vertraulichkeit, als Pensionskassenausweise unverschlossen an Arbeitgebende versandt wurden und damit "in keiner Weise gegen Einsichtnahme oder Kopieren geschützt" waren **2012-14**. Keine Verletzung sah dagegen das Obergericht Zürich im Versand einer E-Mail mit Rechnungs- und Adressdaten ohne Ende-zu-Ende-Verschlüsselung, weil DSG und Verordnung keine bestimmte Verschlüsselungsmethode vorschreiben und die Massnahmen risikobasiert zu wählen sind **UE240472**.

Die Definition löst die Pflichten nach Art. 24 DSG aus, die selbst wieder abgestuft sind: Meldung an den EDÖB nur bei voraussichtlich hohem Risiko, Meldung des Auftragsbearbeiters an den Verantwortlichen bei jeder Verletzung, Information der betroffenen Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt **Art. 24 DSG**. Im Suchmaschinenfall bejahte das Bundesverwaltungsgericht die Informationspflicht wegen des Missbrauchsrisikos, liess aber eine öffentliche Bekanntmachung nach Art. 24 Abs. 5 lit. c DSG genügen, weil eine individuelle Information unverhältnismässig war **a-3790-2024**.

Bundesorgan (lit. i)

Funktionaler Begriff

Bundesorgan ist eine Behörde oder Dienststelle des Bundes oder eine Person, die mit öffentlichen Aufgaben des Bundes betraut ist. Private werden zum Bundesorgan, soweit ihnen solche Aufgaben übertragen sind; das Bundesverwaltungsgericht stellt darauf ab, ob eine private Organisation Verfügungen erlassen kann, wie anerkannte Krankenversicherer oder UVG-Unfallversicherer **a-7367-2006**. Die

SBB gelten als Bundesorgan, weil sie öffentliche Aufgaben erfüllen **a-420-2007**.

Die Eigenschaft ist tätigkeitsbezogen. Handelt ein Bundesorgan privatrechtlich, gelten nach Art. 40 DSG die Bestimmungen für Private **BBl 2020 7639**. Das Bundesverwaltungsgericht hat zum alten, gleichlautenden Recht entschieden, dass für die Abgrenzung auf die Natur des zugrundeliegenden Verhältnisses abzustellen ist: Die mit der Ausgabe des SwissPass verbundene Datenerhebung der SBB war zivilrechtlich, sodass kein Anspruch auf eine Verfügung bestand **a-5921-2020**. Ebenso führten Transportverträge, Ticketshop und Kundendienst zur Zuständigkeit des Zivilgerichts, während für Daten aus dem früheren öffentlich-rechtlichen Arbeitsverhältnis der Verwaltungsrechtsweg offenstand **a-420-2007**. Innerhalb eines Krankenversicherungskonzerns sind nur die Grundversicherer und nur für die obligatorische Krankenpflegeversicherung Bundesorgane; die Zusatzversicherung handelt als Private **a-3548-2018**.

Die Qualifikation hat erhebliche Folgen: Für Bundesorgane gelten das Legalitätsprinzip und die Bekanntgaberegeln der Art. 34 und 36 DSG sowie der Rechtsweg nach Art. 41 DSG **BBl 2020 7639**.

Abgrenzung zu kantonalen Organen

Kantonale und kommunale Organe sind keine Bundesorgane, "même s'ils sont chargés de l'exécution de tâches de la Confédération" (selbst wenn sie mit dem Vollzug von Bundesaufgaben betraut sind); für die kantonale IV-Stelle gilt deshalb das kantonale Datenschutzrecht, und der Rechtsweg führt nicht an das Bundesverwaltungsgericht **1C_125/2015**. Gleiches gilt für Betreibungs- und Konkursämter; das Verwaltungsgericht Graubünden hielt zudem fest, dass Art. 8a SchKG das Einsichtsrecht abschliessend regelt und sowohl DSG als auch kantonales Recht verdrängt **PVG 2020 27**. Das Bundesrecht kann seine Anwendbarkeit aber spezialgesetzlich ausdehnen: Für konzessionierte Transportunternehmen gilt nach Art. 54 PBG das DSG, auch wenn ein Kanton Mehrheitsaktionär ist **ge-2023-0172**.

Verantwortlicher und Auftragsbearbeiter (lit. j und k)

Entscheid über Zweck und Mittel

Verantwortlich ist, wer allein oder zusammen mit anderen über Zweck und Mittel der Bearbeitung entscheidet. Nach der Botschaft entspricht der Verantwortliche dem früheren Inhaber der Datensammlung; die Mittel umfassen etwa materielle oder automatisierte Bearbeitung und verwendete Software **BBl 2017 6941**. Die Rechtsprechung zum alten Recht bleibt deshalb einschlägig: Inhaber war, wer "ohne zwingend über die einzelnen Daten selbst verfügen zu müssen" den Zweck festlegt und die Bearbeitungsmittel bestimmt; auch unverändert von Dritten erworbene Daten gehörten zur Sammlung des Plattformbetreibers, der über ihre Verwendung entschied **a-4232-2015**. Die Verantwortlicheneigenschaft kann aus der Geschäftstätigkeit erschlossen werden, etwa aus der regelmässigen Bekanntgabe von Adressdaten zu Werbezwecken; wer Daten durch Dritte bearbeiten lässt, bleibt auskunftspflichtig **a-5225-2015**.

Die Abgrenzung entscheidet über die Passivlegitimation. Nach dem Kantonsgericht Schwyz verpflichten Art. 8 aDSG und Art. 25 DSG grundsätzlich nur den Verantwortlichen zur Auskunft; wer diese Eigenschaft nicht hat, muss nicht einmal mitteilen, ob er Daten bearbeitet, vorbehältlich der Auftragsbearbeiter nach der Verordnung **ZK1 2023 22**.

Die gemeinsame Verantwortlichkeit ("zusammen mit anderen") ist im Gesetz nur für Bundesorgane näher geregelt: Der Bundesrat regelt Kontrolle und Verantwortung, wenn ein Bundesorgan Daten zusammen mit anderen Bundesorganen, kantonalen Organen oder Privaten bearbeitet **Art. 33 DSG**. Für Private zeigt der Moneyhouse-Entscheid zur gemeinsam geführten Datensammlung die praktische Folge unter altem Recht: Das Auskunftsrecht konnte bei jedem Inhaber geltend gemacht werden, und der nicht zuständige Inhaber musste das Begehren weiterleiten **a-4232-2015**.

Auftragsbearbeiter

Auftragsbearbeiter ist, wer "im Auftrag" des Verantwortlichen Daten bearbeitet. Er entscheidet nicht über den Zweck; nach der Botschaft muss der Verantwortliche aktiv sicherstellen, dass der Auftragsbearbeiter das Gesetz im selben Umfang einhält, und die Aufbewahrung in einer Cloud ist grundsätzlich ein Anwendungsfall der Auftragsbearbeitung **BBl 2017 6941**. Die Übertragung ist zulässig, wenn die Daten nur so bearbeitet werden, wie der Verantwortliche selbst es dürfte, und keine Geheimhaltungspflicht entgegensteht; Unterauftragsbearbeitung bedarf der vorgängigen Genehmigung, und der Auftragsbearbeiter kann dieselben Rechtfertigungsgründe geltend machen **Art. 9 DSG**. Wer eine Bearbeitung ohne Einhaltung dieser Voraussetzungen übergibt, kann sich nach Art. 61 lit. b DSG strafbar machen; das Kantonsgericht Schwyz hob deshalb eine Nichtanhandnahme auf **BEK 2024 84**.

Wer eigene Zwecke verfolgt, ist kein Auftragsbearbeiter. Die Datenlieferanten von Moneyhouse waren nicht Beauftragte, weil das Verhältnis kaufrechtlicher Art war **a-4232-2015**; der Erwerber wurde selbst verantwortlich. Telekommunikationsanbieter, die das städtische Glasfasernetz für eigene Endkundendienste nutzten, erfüllten keine Hilfsfunktion und waren nach kantonalem Recht nicht Auftragsbearbeiter, sondern Empfänger einer Bekanntgabe **VB.2020.00700**. Massgebend ist damit nicht die vertragliche Bezeichnung, sondern wer tatsächlich über Zweck und Mittel bestimmt.

Folgerungen für die Praxis

- Personenbezug dokumentieren. Vor jeder Weitergabe angeblich anonymisierter Daten ist zu prüfen, ob der Empfänger über Zuordnungsmerkmale (AHV-Nummer, Kundennummer, Kontextwissen) verfügt; Pseudonymisierung genügt nicht, wenn der Empfänger die Person bestimmen kann **4A_365/2017**.
- Sensible Kategorien am Inhalt messen. Ob ein Datum unter lit. c fällt, hängt davon ab, was es über die Kategorie aussagt; Stichworte wie "krank" genügen nach der kantonalen Praxis nicht, Einzelheiten zur Art der Krankheit schon **CCP.2010.17**.
- Konzerninterne Flüsse als Bekanntgabe behandeln. Datenflüsse zwischen rechtlich selbständigen Konzerngesellschaften sind als Bekanntgabe zu prüfen und bedürfen eines eigenen Rechtfertigungsgrunds (oben, Bekanntgeben) **a-3548-2018**.
- Rollen festlegen. Für jeden Datenfluss ist zu bestimmen, wer über Zweck und Mittel entscheidet; Datenkäufe und Kooperationen mit Partnern, die eigene Zwecke verfolgen, sind keine Auftragsbearbeitung **a-4232-2015**.
- Öffentlich-rechtliche Tätigkeit trennen. Bundesorgane und beliehene Private sollten ihre Bearbeitungen nach der Natur des Grundverhältnisses ordnen, weil davon Rechtsgrundlage und Rechtsweg abhängen **a-5921-2020**.
- Exponierte Daten als Verletzung prüfen. Schon die Zugänglichkeit für Unbefugte, etwa durch Indexierung, löst die Prüfung der Meldepflicht aus **a-3790-2024**.