Kommentar zu Art. 6 DSG: Grundsätze der Datenbearbeitung

Funktion, Geltungsbereich und Entstehung

Art. 6 DSG fasst die materiellen Bearbeitungsgrundsätze zusammen: Rechtmässigkeit (Abs. 1), Treu und Glauben und Verhältnismässigkeit (Abs. 2), Zweckbindung und Erkennbarkeit (Abs. 3), Speicherbegrenzung (Abs. 4), Richtigkeit (Abs. 5) sowie die Gültigkeit der Einwilligung (Abs. 6 und 7) **Art. 6 DSG**. Das Gesetz konkretisiert nach der Botschaft das Recht auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV, also das Recht, grundsätzlich selbst zu bestimmen, ob und zu welchen Zwecken Daten über die eigene Person bearbeitet werden **BBl 2017 6941**.

Geltungsbereich. Die Grundsätze gelten für jede Bearbeitung von Personendaten natürlicher Personen durch private Personen und Bundesorgane. Ausgenommen sind namentlich die Bearbeitung ausschliesslich zum persönlichen Gebrauch und die Beratungen der eidgenössischen Räte; für Gerichtsverfahren und Verfahren nach bundesrechtlichen Verfahrensordnungen ist das jeweilige Verfahrensrecht massgebend **Art. 2 DSG**. Kantonale Organe unterstehen dem kantonalen Datenschutzrecht; Entscheide zu kantonalem Recht werden hier deshalb nur als Parallelwertungen herangezogen. «Bearbeiten» erfasst jeden Umgang mit Personendaten, vom Beschaffen über das Aufbewahren bis zum Löschen **Art. 5 DSG**.

Kumulative Geltung. Nach dem Bundesverwaltungsgericht enthält Art. 6 DSG für private Bearbeiter wie für Bundesorgane die wesentlichen materiellen Grundsätze; diese «müssen kumulativ eingehalten werden und sind unabhängig voneinander zu prüfen» **a-2941-2024**. Eine Bearbeitung, die einen Grundsatz einhält, kann also an einem anderen scheitern. Im Fall einer öffentlich einsehbaren Datenbank, die im Rahmen einer Kampagne mit einem Fragebogen zu religiösen Themen angefragte Personen mit dem Status «erfasst» oder «angefragt» aufführte, stellte das Gericht nebeneinander Verstösse gegen Verhältnismässigkeit, Zweckbindung und Transparenz fest **a-2941-2024**.

Vorgängerrecht. Abs. 1, 2, 6 und 7 gehen auf Art. 4 aDSG in der Fassung vom 24. März 2006 zurück, Abs. 5 auf Art. 5 aDSG; Abs. 3 vereinigt die früheren Grundsätze der Zweckbindung und der Erkennbarkeit **BBl 2006 3547 BBl 2017 6941**. Die Rechtsprechung zu Art. 4 und 5 aDSG bleibt deshalb für die Auslegung bedeutsam, ist aber jeweils am neuen Wortlaut zu messen. Zur Gesetzgebungsgeschichte der Einwilligungsregeln siehe unten bei Abs. 6 und 7. Seit dem Inkrafttreten am 1. September 2023 ist der Wortlaut von Art. 6 DSG unverändert **DSG (2025-07-07)**.

Übergangsrecht. Art. 69 DSG nimmt für laufende Bearbeitungen nur die Art. 7, 22 und 23 aus, nicht aber Art. 6; die Grundsätze gelten seit dem 1. September 2023 auch für zuvor begonnene Bearbeitungen **Art. 69 DSG**. Für Untersuchungen des EDÖB, die bei Inkrafttreten hängig waren, gilt das bisherige Recht **Art. 70 DSG**. Massgebend ist die formelle Eröffnung der Untersuchung: Vorgängige Korrespondenz und informelle Abklärungen genügten im Datenbank-Fall nicht, sodass neues Recht anwendbar war **a-2941-2024**.

Grundsatzverletzung, Rechtfertigung und gesetzliche Grundlage

Private Bearbeiter: Verstoss als Persönlichkeitsverletzung

Für Private ist Art. 6 DSG mit Art. 30 und 31 DSG zu lesen. Eine Persönlichkeitsverletzung liegt insbesondere vor, wenn Personendaten entgegen den Grundsätzen nach Art. 6 und 8 DSG bearbeitet werden **Art. 30 DSG**. Widerrechtlich ist sie, wenn weder Einwilligung noch überwiegendes privates oder öffentliches Interesse noch Gesetz sie rechtfertigt **Art. 31 DSG**. Der Grundsatzverstoss begründet also die Verletzung; die Rechtfertigung ist eine zweite, eigenständige Prüfungsstufe.

Das Bundesgericht hat zum alten Recht entschieden, dass eine Rechtfertigung von Bearbeitungen entgegen den Grundsätzen zwar nicht generell ausgeschlossen ist, Rechtfertigungsgründe im konkreten Fall aber «nur mit grosser Zurückhaltung bejaht werden können» **BGE 136 II 508 BGE 138 II 346**. Im Fall Logistep, der verdeckten Erfassung von IP-Adressen in Peer-to-Peer-Netzwerken zur Weitergabe an Rechteinhaber, vermochte selbst das Interesse an der wirksamen Bekämpfung von Urheberrechtsverletzungen die Verletzung von Zweckbindung und Erkennbarkeit nicht aufzuwiegen **BGE 136 II 508**. Das Bundesverwaltungsgericht prüft unter neuem Recht nach festgestelltem Verstoss gegen Art. 6 DSG ebenfalls Art. 31 DSG und hat in zwei Internet-Publikationsfällen jeden Rechtfertigungsgrund verneint. Bei der Veröffentlichung mutmasslicher Schuldner fehlten Einwilligung und gesetzliche Grundlage, und den Interessen an der Warnung der Öffentlichkeit und am Inkasso mass das Gericht kein Gewicht bei, weil dafür Strafverfolgung und Schuldbetreibungsrecht zur Verfügung stehen **a-3891-2025**. Bei der religiösen Datenbank deckte Art. 31 Abs. 2 lit. f DSG die Bekanntgabe an Dritte nicht **a-2941-2024**. Wer gegen einen Grundsatz verstösst, kann sich deshalb nur ausnahmsweise auf überwiegende Interessen berufen.

Bundesorgane: gesetzliche Grundlage und Grundsätze nebeneinander

Bundesorgane dürfen Personendaten nur gestützt auf eine gesetzliche Grundlage bearbeiten; für besonders schützenswerte Daten, Profiling und potenziell schwerwiegende Grundrechtseingriffe bedarf es grundsätzlich eines Gesetzes im formellen Sinn **Art. 34 DSG**. Die Einwilligung im Einzelfall ist hier nur ein Ausnahmetatbestand (Art. 34 Abs. 4 lit. b DSG) **Art. 34 DSG**. Das Bundesgericht liess für einen Eintrag im militärmedizinischen Informationssystem MEDISA eine formell-gesetzliche Grundlage im Militärgesetz genügen; dass die betroffene Person vom Eintrag nichts gewusst hatte, änderte an dessen Rechtmässigkeit nichts **1C_524/2024**. Die gesetzliche Grundlage entbindet jedoch nicht von Art. 6 DSG: Das Bundesverwaltungsgericht prüfte bei einer RIPOL-Ausschreibung die Speicherbegrenzung nach Art. 6 Abs. 4 DSG und die Verhältnismässigkeit und hielt die Speicherung bis zum Eintritt der Vollstreckungsverjährung für geeignet, erforderlich und zumutbar **a-7720-2025**.

Rechtmässigkeit (Abs. 1)

Abs. 1 erfasst jede Bearbeitung, nicht nur die Beschaffung **BBl 2003 2101**. Seine Reichweite ist aber begrenzt. Nach dem Bundesverwaltungsgericht ist eine Bearbeitung zu einem rechtswidrigen Zweck erst dann datenschutzrechtlich unrechtmässig, «wenn dabei gegen eine Norm verstossen wird, die zumindest auch, direkt oder indirekt, den Schutz der Persönlichkeit einer Person bezweckt» **a-3548-2018**. Im Fall des Bonusprogramms Helsana+ machte ein allfälliger Verstoss gegen die Prämienvorschriften des KVG die Bearbeitung deshalb nicht unrechtmässig, weil diese Normen dem Grundsatz der Gegenseitigkeit in der sozialen Krankenversicherung dienen und nicht dem Persönlichkeitsschutz **a-3548-2018**.

Derselbe Entscheid zeigt die Gegenrichtung: Die Beschaffung von Daten aus der obligatorischen Krankenpflegeversicherung war unrechtmässig, weil die spezialgesetzlich verlangte Einwilligung fehlte **a-3548-2018** (zu den Formanforderungen unten bei Abs. 7). Spezialgesetzliche Anforderungen an Einwilligungen und Bekanntgaben wirken somit über Abs. 1 in das DSG hinein. Der Entscheid erging zu Art. 4 Abs. 1 aDSG, dessen Wortlaut Art. 6 Abs. 1 DSG übernimmt.

Treu und Glauben, Transparenz und Zweckbindung (Abs. 2 und 3)

Erkennbarkeit von Beschaffung und Zweck

Abs. 3 verlangt einen bestimmten und für die betroffene Person erkennbaren Zweck. Nach der Botschaft müssen sowohl die Beschaffung als auch der Bearbeitungszweck erkennbar sein, und vage, nicht definierte oder unpräzise Zwecke genügen nicht **BBl 2017 6941**. Der Transparenzgrundsatz ist eng mit Treu und Glauben (Abs. 2) verbunden: Nach dem Bundesgericht müssen die Betroffenen zur Durchsetzung des Datenschutzes zunächst wissen, ob Daten über sie bearbeitet werden **BGE 148 II 349**. Die Informationspflicht nach Art. 19 DSG konkretisiert dies und verlangt mindestens Angaben zur Identität des Verantwortlichen, zum Zweck und zu den Empfängern **Art. 19 DSG**. Sind Beschaffung und Zweck nach den konkreten Umständen offensichtlich erkennbar, ist nach den Materialien zur Revision 2006 keine zusätzliche Information nötig **BBl 2003 2101**.

Die Rechtsprechung stellt an die Erkennbarkeit konkrete Anforderungen:

- Zeitpunkt. «Eine nachträgliche Information genügt den Anforderungen an die Transparenz nicht.» **a-3891-2025** Es reicht auch nicht, dass Betroffene sich nach einer Veröffentlichung selbst beim Bearbeiter melden **a-3891-2025**.
- Konkretheit. Ein blosser Link auf eine Website machte die Publikation von Statusdaten nicht erkennbar **a-2941-2024**. Bei Google Street View genügte die Sichtbarkeit der Kamerafahrzeuge nicht: «Ob ein vorbeifahrendes Google-Fahrzeug gerade Aufnahmen tätigt, ist für die Anwesenden nicht erkennbar.» **BGE 138 II 346** Eine Internetinformation eine Woche im Voraus über die aufzunehmenden Gebiete gewährleistete die Erkennbarkeit nicht hinreichend **BGE 138 II 346**.
- Heimliche Aufnahmen. Aufnahmen einer Dashcam sind für andere Verkehrsteilnehmer nicht ohne Weiteres erkennbar: «Die Datenbearbeitung ist damit als heimlich im Sinne von Art. 4 Abs. 4 DSG zu qualifizieren.» **BGE 146 IV 226** (gemeint ist das aDSG) Hinweise am Fahrzeug ändern daran nichts, weil von Fahrzeugführern nicht erwartet werden kann, nach solchen Hinweisen Ausschau zu halten **BGE 146 IV 226**.

Grenzen. Transparenz kann auch durch Gesetz hergestellt werden. Bei Datenübermittlungen in der Steueramtshilfe entfiel die vorgängige Informationspflicht, weil die spezialgesetzlichen Bestimmungen für nicht direkt betroffene Dritte genügend erkennen lassen, dass Daten beschafft und weitergegeben werden können **BGE 148 II 349**. Das neue Recht kennt entsprechende Ausnahmen von der Informationspflicht, etwa bei gesetzlich vorgesehener Bearbeitung oder wenn die Information den Zweck der Bearbeitung vereiteln würde **Art. 20 DSG**. Im Arbeitsverhältnis wurde Transparenz durch ein Nutzungsreglement und wiederholte Warnhinweise beim Sperren unzulässiger Websites hergestellt; eine anonyme, statistische Auswertung von Internet-Protokolldaten war unter diesen Voraussetzungen zulässig **a-6453-2014**.

Vorhersehbarkeit der Folgeverwendung (kantonale Parallele). Wie die Erkennbarkeit auch ohne ausdrückliche Information aus dem Sachzusammenhang folgen kann, zeigt ein Urteil der Waadtländer Cour de droit administratif et public zum kantonalen Datenschutzgesetz (LPrD), das Art. 6 DSG nicht anwendet. Eine Gemeinde verlangte von der kantonalen Energiebehörde die Liste der Gebäude auf ihrem Gebiet, die 2022 bis 2024 Energiesubventionen erhalten hatten, um die Einhaltung der Bau- und Brandschutzbewilligungen zu kontrollieren. Das Gericht prüfte die Erkennbarkeit im Einzelfall und hielt sie für gegeben, weil die Subvention für Arbeiten am Gebäude beantragt wird, «pour lesquels le requérant ne peut pas ignorer qu'une autorisation communale pourrait être nécessaire» (für die der Gesuchsteller nicht übersehen kann, dass eine Gemeindebewilligung nötig sein könnte) **ge-2026-0008**. Auch den Kontrollzweck der Gemeinde erachtete es als vereinbar mit dem ursprünglichen Beschaffungszweck, sodass die Bekanntgabe weder den Grundsatz der Zweckbindung noch jenen der Transparenz verletzte **ge-2026-0008**. Die Grenze zog das Gericht bei der Verhältnismässigkeit: Unzulässig wäre eine «recherche généralisée et indéterminée de moyens de preuve» (eine allgemeine und unbestimmte Beweissuche), die hier wegen der zeitlichen, örtlichen und sachlichen Beschränkung der Anfrage nicht vorlag **ge-2026-0008**. Ob und wie die Betroffenen nachträglich zu informieren sind und ob ihnen ein Widerspruchsrecht zusteht, entschied das Gericht nicht selbst, sondern wies diese Frage an die kantonale Datenschutzbehörde zurück **ge-2026-0008**. Als Parallelwertung stützt der Entscheid den Gedanken, dass eine für die betroffene Person vorhersehbare Folgeverwendung erkennbar sein kann, beantwortet die Frage der Informationspflicht aber nicht.

Vereinbarkeit der Weiterbearbeitung

Die Weiterbearbeitung muss mit dem Beschaffungszweck vereinbar sein. Nach der Botschaft ist sie unzulässig, wenn die betroffene Person sie «berechtigterweise als unerwartet, unangebracht oder beanstandbar erachten kann» **BBl 2017 6941**. Unvereinbar ist danach etwa die Werbenutzung von Adressen, die beim Unterschriftensammeln für eine politische Kampagne erfasst wurden; vereinbar ist dagegen die Werbung eines Unternehmens an eine Adresse, die für eine Kundenkarte oder eine Bestellung angegeben wurde **BBl 2017 6941**. Eine Zweckänderung kann auch durch Gesetz oder einen anderen Rechtfertigungsgrund wie die Einwilligung gedeckt sein **BBl 2017 6941**.

Allgemein zugängliche Daten sind kein Freibrief. Art. 30 Abs. 3 DSG schliesst eine Persönlichkeitsverletzung nur in der Regel aus, wenn die betroffene Person die Daten selbst allgemein zugänglich gemacht und die Bearbeitung nicht ausdrücklich untersagt hat **Art. 30 DSG**. Das Bundesverwaltungsgericht hielt fest, dass davon die Kontaktaufnahme mit den Betroffenen gedeckt war, nicht aber die Weiterverarbeitung in einem neuen Kontext, nämlich die öffentliche Anzeige ihres Status «erfasst» oder «angefragt» **a-2941-2024**. Als Gegenbeispiel bewegte sich die unveränderte und zeitlich unbeschränkte Weiterverbreitung von Handelsregisterdaten durch einen privaten Anbieter innerhalb des gesetzlichen Zwecks des Handelsregisters **2008-16**. Entscheidend ist somit, ob der neue Verwendungskontext noch vom ursprünglich erkennbaren Zweck getragen wird.

Verhältnismässigkeit (Abs. 2)

Nach der Botschaft dürfen nur Daten bearbeitet werden, die für den Zweck geeignet und nötig sind; die Rechte der Betroffenen sind so weit wie möglich zu wahren, und Datenvermeidung und Datensparsamkeit sind Ausdruck dieses Grundsatzes **BBl 2017 6941**. Art. 7 DSG setzt dies organisatorisch um: Die Bearbeitung ist ab der Planung so auszugestalten, dass insbesondere die Grundsätze nach Art. 6 eingehalten werden, und Voreinstellungen müssen sie auf das für den Verwendungszweck nötige Mindestmass beschränken **Art. 7 DSG**.

Die Prüfung folgt dem dreistufigen Schema aus Eignung, Erforderlichkeit (Wahl des mildesten von mehreren geeigneten Mitteln) und Verhältnismässigkeit im engeren Sinn **BGE 130 II 425**. Die Erforderlichkeit ist in der Praxis meist ausschlaggebend:

- Die Veröffentlichung mutmasslicher Schuldner im Internet war nicht das mildeste Mittel zur Zweckerreichung, weil Schuldbetreibungsrecht und Strafverfolgung zur Verfügung standen **a-3891-2025**.
- Bei der religiösen Datenbank war die öffentliche Anzeige des Status für die Zielerreichung «nicht aussagekräftig» **a-2941-2024**.
- Bei Anmeldeformularen für Mietwohnungen prüfte die Eidgenössische Datenschutzkommission jede einzelne Angabe: Name der bisherigen Verwaltung und aktueller Mietzins waren für den Abschlussentscheid nicht nötig und ihre Erhebung unverhältnismässig, während für Angaben zur Aufenthaltsbewilligung und zu Betreibungen in den gesetzlichen Grenzen ein überwiegendes Interesse bestand **150006365**.

Die Verhältnismässigkeit wird oft durch Auflagen und nicht durch ein Verbot hergestellt. Bei Street View liess das Bundesgericht eine Fehlerquote von etwa 1 % bei der automatischen Anonymisierung zu, verlangte aber eine vollständige Anonymisierung vor sensiblen Einrichtungen wie Frauenhäusern, Altersheimen, Gefängnissen, Schulen, Gerichten und Spitälern und untersagte die Publikation von Privatbereichen, die aus einer Kamerahöhe von über 2 m aufgenommen wurden und einem gewöhnlichen Passanten verschlossen bleiben **BGE 138 II 346**.

Typische Anwendungsfelder von Abs. 2 und 3

Überwachung im Arbeitsverhältnis

Im Arbeitsverhältnis darf der Arbeitgeber Daten nur bearbeiten, soweit sie die Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind; im Übrigen gilt das DSG **Art. 328b OR**. Hinzu tritt das Verbot von Überwachungssystemen, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen **Art. 26 ArGV 3**. Das Bundesgericht legt dieses Verbot einschränkend aus: Untersagt sind Systeme, die ausschliesslich oder hauptsächlich das Verhalten als solches überwachen; aus legitimen Gründen wie Sicherheit oder Arbeitsorganisation eingesetzte Systeme sind zulässig, sofern sie verhältnismässig sind und die Arbeitnehmer vorgängig informiert wurden **BGE 130 II 425**. Ein GPS-System in Dienstfahrzeugen war danach zulässig, weil die Überwachung nur mittelbar (über die Fahrzeuge), auf die Ortswechsel beschränkt und nicht dauernd war; eine kontinuierliche Verfolgung in Echtzeit hätte dagegen unverhältnismässig sein können **BGE 130 II 425**.

Die Gegenbeispiele zeigen die Grenzen. Die verdeckte Installation einer Spyware, die während über drei Monaten die gesamte Computeraktivität eines Angestellten aufzeichnete, war unverhältnismässig, weil eine summarische Auswertung vorhandener Logfiles und eine Ermahnung genügt hätten **BGE 139 II 7**. Ein Zürcher Arbeitsgericht erklärte die GPS-Überwachung eines auch privat nutzbaren Dienstwagens für unzulässig, obwohl der Arbeitnehmer auf das GPS hingewiesen worden war, weil das Gerät alle Bewegungen ohne Unterscheidung zwischen beruflicher und privater Nutzung aufzeichnete und der Arbeitgeber keine Schutzvorkehren getroffen hatte **AH180153-L**. Die Information über das System beseitigt somit die Unverhältnismässigkeit nicht.

Videoüberwachung durch Private

Private Videoüberwachung identifizierbarer Personen untersteht dem DSG und muss Treu und Glauben, Verhältnismässigkeit und Erkennbarkeit wahren **6B_768/2022**. Das Bundesgericht verlangt, dass die Personen informiert werden, bevor sie in das Kamerafeld treten, und hält fest: «Un système de vidéosurveillance privé qui filme l'espace public sera généralement jugé disproportionné et, donc, illicite.» (Ein privates Videoüberwachungssystem, das den öffentlichen Raum filmt, wird in der Regel als unverhältnismässig und damit widerrechtlich beurteilt.) **6B_768/2022** Weil die Vorinstanz weder die Sichtbarkeit von Kamera und Hinweisschild vor dem Betreten des Erfassungsbereichs noch mildere Massnahmen abgeklärt hatte, wies das Bundesgericht die Sache zurück **6B_768/2022**.

Die Genfer Beschwerdekammer verweist auf die Praxis des EDÖB, wonach Private aus Praktikabilitätsgründen einen kleinen Teil des öffentlichen Raums miterfassen dürfen, wenn sich das private Grundstück nicht anders schützen lässt; auch sie wies mangels Sachverhaltsabklärung zum Zweck und zur Erkennbarkeit zurück **ACPR/685/2023**. Das Waadtländer Kantonsgericht beurteilte dagegen eine Kamera, die den gemeinsamen Vorplatz einer Überbauung und den Sichtschutz des Nachbargartens erfasste, als widerrechtlich; die kurze Speicherdauer von 24 Stunden änderte daran nichts, und mildere Mittel wie Verschlüsse oder eine Alarmanlage waren nicht als untauglich nachgewiesen **CACI pp20-043408-542/2022**. Diese Entscheide ergingen noch zum aDSG.

Speicherbegrenzung und Anonymisierung (Abs. 4)

Personendaten sind zu vernichten oder zu anonymisieren, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind **Art. 6 DSG**. Nach der Botschaft bedingt die Einhaltung dieser Pflicht, «dass der Verantwortliche Aufbewahrungsfristen festlegt» **BBl 2017 6941**. Nach dem Wortlaut («sobald») ist die Pflicht vom Verantwortlichen selbst zu erfüllen und setzt kein Gesuch der betroffenen Person voraus **Art. 6 DSG**.

Gesetzliche Aufbewahrungspflichten. Spezialgesetzliche Aufbewahrungsfristen bleiben vorbehalten **BBl 2017 6941**. So sind Geschäftsbücher und Buchungsbelege während zehn Jahren aufzubewahren **Art. 958f OR**, und Protokolle nach Art. 4 DSV sind mindestens ein Jahr aufzubewahren und dürfen nur für die Überprüfung des Datenschutzes und der Datensicherheit verwendet werden **Art. 4 DSV**. Solche Pflichten definieren den Zweck der weiteren Aufbewahrung und begrenzen zugleich die zulässige Verwendung der Daten.

Massstab der Erforderlichkeit. Die Rechtsprechung beurteilt die Erforderlichkeit funktional. Nach dem Bundesgericht ist bei Polizeidaten entscheidend, ob sie der polizeilichen Arbeit «in nachvollziehbarer Weise noch nützlich sein können und die weitere Aufbewahrung im öffentlichen Interesse ist»; die Einstellung des Strafverfahrens erzwingt deshalb keine sofortige Löschung, wenn der Eintrag die Einstellung klar ausweist und die automatische Löschung absehbar ist **1C_439/2011**. Der Europäische Gerichtshof für Menschenrechte hielt dagegen die jahrelange Beibehaltung der unbelegten Bezeichnung «prostituée» in einem Genfer Polizeidossier für nicht notwendig in einer demokratischen Gesellschaft, weil der Verdacht vage und nicht durch konkrete Tatsachen gestützt war **16188/07**. Für kantonale Polizeidaten haben die Verwaltungsgerichte Zürich (zehnjährige Löschfrist bei Gewaltschutzverfahren) und Bern (fünfjährige Aufbewahrung eines Journaleintrags) die Aufbewahrung nach kantonalem Recht als verhältnismässig bestätigt **VB.2024.00039 100 2023 166**. Für Bundesorgane gilt Abs. 4 direkt, wie der

RIPOL-Fall zeigt (oben) **a-7720-2025**.

Anforderungen an die Anonymisierung. Anonymisierung ist nach dem Bundesgericht jede Massnahme, die bewirkt, dass die Identität der betroffenen Person nicht mehr oder nur noch mit ausserordentlichem Aufwand festgestellt werden kann **1C_425/2020**. Daten, die eine AHV-Nummer enthielten und sich über ein Adressverzeichnis verknüpfen liessen, waren deshalb nicht anonymisiert **1C_425/2020**. Eine Pseudonymisierung genügt nur, wenn sie nicht reversibel ist; wer sich auf die Wirksamkeit der Pseudonymisierung beruft, trägt dafür die Beweislast **4A_365/2017**. Nach der Botschaft fällt aus dem Anwendungsbereich nur, was nicht oder nur mit einem Aufwand reidentifizierbar ist, den kein Interessent auf sich nehmen würde; dies gilt auch für pseudonymisierte Daten **BBl 2017 6941**. Werden die Daten weiterhin personenbezogen benötigt, ist die Anonymisierung kein taugliches milderes Mittel **100 2023 166**.

Richtigkeit (Abs. 5)

Vergewisserungspflicht und angemessene Massnahmen

Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern und alle angemessenen Massnahmen treffen, damit unrichtige oder unvollständige Daten berichtigt, gelöscht oder vernichtet werden; die Angemessenheit hängt namentlich von Art und Umfang der Bearbeitung sowie vom Risiko für die Persönlichkeit oder die Grundrechte ab **Art. 6 DSG**. Gegenüber Art. 5 aDSG sind das Löschen und dieser Risikomassstab neu ausdrücklich genannt **BBl 2006 3547**. Nach der Botschaft ist der Umfang der Vergewisserungspflicht im Einzelfall zu bestimmen, und Daten, die nicht korrigiert oder ergänzt werden können, sind zu löschen oder zu vernichten **BBl 2017 6941**.

Wie weit die Pflicht reichen kann, zeigt der Moneyhouse-Entscheid: Das Bundesverwaltungsgericht verpflichtete die Betreiberin einer Wirtschaftsauskunftsplattform, ihren Datenbestand im Verhältnis von 5 % zu den getätigten Abfragen auf Richtigkeit zu überprüfen **a-4232-2015**. Bei massenhaften Bearbeitungen mit hohem Risiko verlangt Abs. 5 somit systematische Stichprobenkontrollen. Unrichtig sind Daten, die nicht mit der Realität übereinstimmen, veraltet oder unvollständig sind; ein Eintrag, der den Erkenntnisstand im Zeitpunkt der Erfassung korrekt wiedergibt, ist nach dem Zürcher Verwaltungsgericht nicht unrichtig **VB.2024.00039**.

Grenzen. Nach der Botschaft können gesetzliche Pflichten der Berichtigung, Löschung oder Aktualisierung entgegenstehen, und für Archive, Museen und andere Gedächtnisinstitutionen ist der Grundsatz differenziert zu betrachten **BBl 2017 6941**. Der Berichtigungsanspruch nach Art. 32 Abs. 1 DSG ist ausgeschlossen, wenn eine gesetzliche Vorschrift die Änderung verbietet oder die Daten zu Archivzwecken im öffentlichen Interesse bearbeitet werden **Art. 32 DSG**. Akten eines abgeschlossenen Justizverfahrens können nach dem Aargauer Verwaltungsgericht nur nach Prozessrecht geändert werden; Parteibehauptungen in Rechtsschriften unterliegen keinem datenschutzrechtlichen Berichtigungsanspruch **WBE.2022.152**.

Beweislast, Berichtigung und Bestreitungsvermerk

Für Bundesorgane hat das Bundesverwaltungsgericht die Beweislast verteilt: Die gesuchstellende Person hat die Richtigkeit der verlangten Änderung, die Bundesbehörde im Bestreitungsfall die Richtigkeit der von ihr bearbeiteten Daten zu beweisen **d-3102-2025 a-5104-2024**. Gelingt keiner Partei der Nachweis, sind die wahrscheinlicheren Daten einzutragen oder zu belassen und mit einem Bestreitungsvermerk nach Art. 41 Abs. 4 DSG zu versehen **d-3102-2025 Art. 41 DSG**. Die beiden ZEMIS/SYMIC-Entscheide zum Geburtsdatum zeigen die Spannweite: In einem Fall erschien das vom Gesuchsteller geltend gemachte Datum zumindest nicht weniger wahrscheinlich, sodass das SEM angewiesen wurde, es einzutragen **d-3102-2025**; im anderen blieb das verlangte Datum unbewiesen, der Eintrag wurde belassen, aber mit einem Bestreitungsvermerk versehen **a-5104-2024**. Für Bestände von Gedächtnisinstitutionen sind Berichtigung und Bestreitungsvermerk ausgeschlossen **Art. 41 DSG**.

Gegenüber Privaten kann die klagende Partei einen Bestreitungsvermerk verlangen, wenn weder Richtigkeit noch Unrichtigkeit festgestellt werden kann **Art. 32 DSG**. Die Genfer Cour de justice hielt in einem Bankfall fest, dass der Bearbeiter nachweisen muss, die nötigen Massnahmen zur Sicherung der Richtigkeit getroffen zu haben, während die gesuchstellende Person die Unrichtigkeit beweisen muss; weil der Eintrag als wirtschaftlich Berechtigter richtig war und kein vernünftiger Zweifel bestand, wurden Berichtigung und Bestreitungsvermerk abgelehnt **ACJC/805/2025**. Der Bestreitungsvermerk setzt somit einen echten Beweisnotstand voraus.

Einwilligung (Abs. 6 und 7)

Funktion: Gültigkeitsregel, kein allgemeines Einwilligungserfordernis

Abs. 6 setzt voraus, dass eine Einwilligung «erforderlich» ist, und regelt nur deren Gültigkeit **Art. 6 DSG**. Das DSG macht die Einwilligung nicht zur allgemeinen Voraussetzung jeder Bearbeitung. Für Private ist sie einer von mehreren Rechtfertigungsgründen einer Persönlichkeitsverletzung **Art. 31 DSG**; für Bundesorgane ersetzt sie die gesetzliche Grundlage nur ausnahmsweise im Einzelfall **Art. 34 DSG**. Erforderlich wird sie, wenn ohne sie eine widerrechtliche Persönlichkeitsverletzung vorläge oder wenn ein Spezialgesetz sie verlangt, wie im Fall Helsana+ das KVG **a-3548-2018**. Nach der Botschaft muss die Einwilligung den Zweck abdecken, für den sie als Rechtfertigungsgrund dient; Bearbeitungen zu weiteren Zwecken bedürfen einer anderen Rechtfertigung **BBl 2017 6941**.

Bestimmtheit und angemessene Information

Die Einwilligung muss sich auf eine oder mehrere bestimmte Bearbeitungen beziehen. Das Bundesverwaltungsgericht folgert daraus: «Eine globale Einwilligung in Bezug auf unbestimmte Bearbeitungen oder Bearbeitungen für beliebige Zwecke ist damit ungültig.» **a-2941-2024** Zur Information genügt, dass sich die betroffene Person «im Klaren darüber sein kann, worin sie einwilligen soll, d.h. was die Tragweite ihrer Entscheidung ist» **a-3908-2008**. Nach den Materialien zur Revision 2006 gehört dazu auch die Information über mögliche negative Folgen einer Verweigerung **BBl 2003 2101**. Bei sensiblen Daten steigen die Anforderungen: Für biometrische Daten müsste die Information umfassend sein; ein Informationsblatt, das nicht ordnungsgemäss abgegeben wurde, genügte nicht **a-3908-2008**.

Allgemeine Geschäftsbedingungen schliessen eine gültige Einwilligung nicht aus. Das Bundesgericht hielt die Einwilligung eines Nutzers in die Datenbearbeitung durch Instagram über Nutzungsbedingungen und Datenschutzrichtlinien für gültig, weil sie «auf hinreichend zur Kenntnis gebrachten und für ihn genügend erkennbaren Angaben» beruhte **6B_219/2022**. Umgekehrt erklärte das Waadtländer Kantonsgericht eine generelle Vollmacht in der Sozialhilfe für ungültig, weil die betroffene Person den Kreis der zur Auskunft ermächtigten Personen und Stellen nicht hinreichend abschätzen konnte **ps-2008-0073**. Beide Entscheide ergingen unter früherem Recht.

Freiwilligkeit, Koppelung und Abhängigkeit

Freiwillig ist die Einwilligung nur, wenn der betroffenen Person «eine - mit nicht unzumutbaren Nachteilen behaftete - Handlungsalternative» zur Verfügung steht **a-3908-2008**. Wird eine Alternative erst nach der Weigerung angeboten, fehlt es an der Freiwilligkeit **a-3908-2008**.

Die Koppelung einer Leistung an die Einwilligung ist nicht per se

unzulässig. Im Fall Helsana+ war die Einwilligung freiwillig, weil der Nachteil bei Verweigerung, nämlich die Unmöglichkeit der Teilnahme am Bonusprogramm, einen direkten Bezug zu den Daten aufwies, für deren Bearbeitung eingewilligt wurde **a-3548-2018**. Massgebend ist somit der Sachzusammenhang zwischen verweigerter Leistung und Datenbearbeitung.

In Abhängigkeitsverhältnissen wird die Freiwilligkeit regelmässig verneint. Lernende, die wussten, dass die Verweigerung eines Drogentests als Vertragsverletzung gewertet würde, gaben keine wirklich freiwillige Einwilligung; die Eidgenössische Datenschutzkommission liess offen, ob dies vor Antritt der Lehrstelle noch anders zu beurteilen wäre, schloss es für Tests während der Lehrzeit aber aus **150006614**. Wohnungssuchende sind in ihrer Freiheit, die Erhebung bestimmter Daten zu verweigern, faktisch eingeschränkt, sodass das Ausfüllen eines Anmeldeformulars keine gültige Einwilligung darstellt **150006365**. Auch die Androhung einer Kürzung der Sozialhilfe um 25 % bis zur Unterzeichnung einer Vollmacht schloss eine freie Einwilligung aus **ps-2008-0073**. Im Arbeitsverhältnis verlangte die Genfer Cour d'appel des prud'hommes für die Kontaktaufnahme des Arbeitgebers mit dem künftigen Arbeitgeber eine unmissverständliche Einwilligung der Arbeitnehmerin; ein blosser Hinweis in einer Zeugenaussage genügte nicht **CAPH/19/2023**. In solchen Konstellationen ist die Bearbeitung daher auf einen anderen Rechtfertigungsgrund, etwa Art. 328b OR, zu stützen.

Form: stillschweigende, ausdrückliche und spezialgesetzliche Einwilligung

Ausserhalb von Abs. 7 ist die Einwilligung formfrei. Nach der Botschaft kann sie auch stillschweigend erfolgen, doch «blosses Schweigen oder Untätigkeit» gilt nicht als gültige Einwilligung in eine Persönlichkeitsverletzung **BBl 2017 6941**. Der bundesrätliche Entwurf verlangte zusätzlich eine «eindeutige» Einwilligung; der Nationalrat strich dieses Wort mit dem Mehrheitsantrag, wonach die Einwilligung «nach angemessener Information freiwillig erteilt» werden muss, ohne dass die Debatte eine besondere Begründung für diese Streichung festhält **AB 2019 N 1775**. Die Botschaftspassagen zur «Eindeutigkeit» sind daher nur noch eingeschränkt verwertbar; am Ausschluss blossen Schweigens ändert die Streichung nach dem Gesetzeswortlaut, der eine «erteilte» Einwilligung verlangt, nichts.

Ausdrücklichkeit nach Abs. 7. Eine ausdrückliche Einwilligung ist erforderlich für besonders schützenswerte Personendaten (lit. a), für ein Profiling mit hohem Risiko durch eine private Person (lit. b) und für jedes Profiling durch ein Bundesorgan (lit. c) **Art. 6 DSG**. Wo eine ausdrückliche Einwilligung verlangt ist, kann sie nicht stillschweigend gegeben werden **BBl 2017 6941**. Ein separates Formular ist dagegen nicht nötig: Das Bundesverwaltungsgericht liess eine ausdrückliche Einwilligung genügen, die mit der Unterzeichnung einer Vertragsklausel erteilt wurde **b-5181-2018**. Der EDÖB verlangt für ausdrückliche Einwilligungen über Cookie-Banner Schaltflächen oder Felder, die ein aktives Anklicken erfordern **EDÖB Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien**; dies ist nicht bindende Verwaltungspraxis.

Spezialgesetzliche Formvorschriften gehen weiter. Im Fall Helsana+ verlangte das KVG für die Bekanntgabe von Daten der Grundversicherung eine schriftliche Einwilligung im Einzelfall; das Anklicken einer Schaltfläche in der App genügte mangels eigenhändiger Unterschrift nicht **a-3548-2018**.

Profiling mit hohem Risiko (Abs. 7 lit. b und c)

Profiling ist jede automatisierte Bearbeitung, um persönliche Aspekte einer natürlichen Person zu bewerten; ein Profiling mit hohem Risiko liegt vor, wenn es zu einer Verknüpfung von Daten führt, «die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt» **Art. 5 DSG**. Die Regel ist ein Kompromiss: Der Bundesrat wollte für jedes Profiling eine ausdrückliche Einwilligung, der Nationalrat in keinem Fall; der Ständerat setzte einen risikobasierten Ansatz durch **AB 2019 S 1240**. Die Einigungskonferenz übernahm diese Lösung, nachdem Bundesrat, Verwaltung und EDÖB versichert hatten, dass sie gegenüber der bisherigen Rechtslage und der Anwendung der Moneyhouse-Rechtsprechung keine Verschärfung bewirke **AB 2020 N 1817**. Der Kommissionssprecher hielt fest, dass man «bei der Bemessung» nicht über das Moneyhouse-Urteil hinausgehen solle **AB 2020 N 1817**.

Damit wird der Moneyhouse-Entscheid zum Auslegungsanker für lit. b. Das Bundesverwaltungsgericht hatte dort zum früheren Begriff des Persönlichkeitsprofils entschieden, dass die systematische Verknüpfung von Identifikationsdaten mit Angaben zu den privaten Lebens- und Wohnverhältnissen, teils mit früheren Wohnorten und beruflichen Daten, ein Persönlichkeitsprofil ergab, für das die notwendige explizite Einwilligung nicht belegt war **a-4232-2015**. Für Bundesorgane gilt die Ausdrücklichkeit für jedes Profiling (lit. c), was mit dem Erfordernis einer formell-gesetzlichen Grundlage für Profiling nach Art. 34 Abs. 2 lit. b DSG korrespondiert **Art. 34 DSG**. Ein Profiling mit hohem Risiko schliesst zudem die Rechtfertigung der Bonitätsprüfung nach Art. 31 Abs. 2 lit. c DSG aus **Art. 31 DSG**.

Widerruf

Die Einwilligung ist nicht endgültig. Bereits ein Gutachten unter früherem Recht hielt fest: «Il peut être retiré en tout temps.» (Sie kann jederzeit widerrufen werden.) **150001781** Die Einwilligung kann von vornherein oder nachträglich eingeschränkt werden; bei einem Widerruf zur Unzeit, etwa kurz vor einer Ausstrahlung, bleibt Schadenersatz vorbehalten **150001781**. Nach dem Widerruf ist eine weitere Bearbeitung nicht mehr durch die Einwilligung gedeckt **150001781** und kann zudem gegen eine ausdrückliche Willenserklärung im Sinne von Art. 30 Abs. 2 lit. b DSG verstossen **Art. 30 DSG**. Spezialgesetze können verlangen, dass auf die Widerrufbarkeit hingewiesen wird; das Bundesverwaltungsgericht ordnete im Arbeitsvermittlungsrecht eine entsprechende Ergänzung einer Vertragsklausel an **b-5181-2018**.

Einwilligungsfähigkeit

Die Einwilligung setzt Urteilsfähigkeit voraus. Das Bundesgericht hat für die Einwilligung in medizinische Behandlungen entschieden, dass urteilsfähige Minderjährige höchstpersönliche Rechte selbst ausüben und von den Eltern nur bei Urteilsunfähigkeit vertreten werden: «Le mineur ne sera donc représenté par ses parents que s'il est incapable de discernement» (Der Minderjährige wird somit nur dann von seinen Eltern vertreten, wenn er urteilsunfähig ist) **BGE 134 II 235**. Ob die datenschutzrechtliche Einwilligung stets als höchstpersönliches Recht in diesem Sinn gilt, entscheidet dieses Urteil nicht; es spricht aber dafür, bei urteilsfähigen Minderjährigen deren eigene Einwilligung einzuholen, jedenfalls wenn die Bearbeitung ihre Persönlichkeit wesentlich berührt.

Cookies und ähnliche Technologien

Bei Cookies tritt Art. 45c FMG neben das DSG: Die Bearbeitung von Daten auf fremden Geräten ist ausserhalb der Fernmeldedienste nur zulässig, wenn die Benutzer über Bearbeitung und Zweck informiert und auf die Ablehnungsmöglichkeit hingewiesen werden **Art. 45c FMG**. Nach dem Leitfaden des EDÖB ersetzt diese Norm die Anforderungen des DSG nicht; für nicht notwendige Cookies mit hoher Eingriffsintensität, namentlich bei besonders schützenswerten Daten oder Profiling mit hohem Risiko, sei vor der Bearbeitung eine ausdrückliche Einwilligung einzuholen **EDÖB Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies**. Ein Dialogfeld, das nur die Wahl zwischen der Annahme aller Cookies und dem Verzicht auf die Website lässt, versteht der EDÖB nicht als gültige Willenserklärung **EDÖB Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies**. Diese Aussagen geben die Praxis der Aufsichtsbehörde wieder und binden die Gerichte nicht.

Rechtsfolgen und Durchsetzung

Zivilrechtliche Ansprüche

Gegenüber Privaten richten sich die Klagen nach Art. 28 ff. ZGB; die klagende Partei kann insbesondere das Verbot einer Bearbeitung oder Bekanntgabe sowie die Löschung oder Vernichtung der Daten verlangen, ferner die Berichtigung unrichtiger Daten und die Mitteilung oder Veröffentlichung des Urteils an Dritte **Art. 32 DSG**. Gegenüber Bundesorganen kann verlangt werden, dass die widerrechtliche Bearbeitung unterlassen, ihre Folgen beseitigt oder ihre Widerrechtlichkeit festgestellt wird; statt der Löschung ist die Bearbeitung in bestimmten Fällen einzuschränken, und das Verfahren richtet sich nach dem VwVG **Art. 41 DSG**.

Aufsichtsrechtliche Massnahmen und Strafrecht

Der EDÖB eröffnet eine Untersuchung von Amtes wegen oder auf Anzeige, wenn genügend Anzeichen für einen Verstoss bestehen; bei geringfügigen Verletzungen kann er davon absehen **Art. 49 DSG**. Stellt er eine Verletzung fest, kann er die Anpassung, Unterbrechung oder den Abbruch der Bearbeitung sowie die Löschung oder Vernichtung der Daten verfügen; hat der Bearbeiter während der Untersuchung den rechtmässigen Zustand wiederhergestellt, kann er sich auf eine Verwarnung beschränken **Art. 51 DSG**. In beiden Internet-Publikationsfällen bestätigte das Bundesverwaltungsgericht entsprechende Verfügungen **a-3891-2025 a-2941-2024**.

Ein Verstoss gegen Art. 6 DSG ist als solcher nicht strafbar. Die Strafbestimmungen erfassen nur bestimmte Pflichtverletzungen, namentlich vorsätzliche Verletzungen der Informations-, Auskunfts- und Mitwirkungspflichten, bestimmter Sorgfaltspflichten und der beruflichen Schweigepflicht **Art. 60 DSG Art. 61 DSG Art. 62 DSG**. Mittelbar kann eine intransparente Bearbeitung aber strafbar werden, wenn zugleich die Informationspflicht nach Art. 19 DSG vorsätzlich verletzt wird **Art. 60 DSG**.

Verwertbarkeit grundsatzwidrig beschaffter Beweismittel

Daten, die unter Verletzung von Art. 6 DSG erhoben wurden, sind rechtswidrig beschafft. Im Zivilprozess werden sie nur berücksichtigt, wenn das Interesse an der Wahrheitsfindung überwiegt **Art. 152 ZPO**. Das Bundesgericht verlangt eine restriktive Handhabung und bestätigte den Ausschluss der Abschrift einer heimlichen Tonaufnahme, weil in einem rein vermögensrechtlichen Privatstreit die finanziellen Interessen den Schutz der Privatsphäre nicht überwogen; die Abwägung der Vorinstanz überprüft es nur zurückhaltend **4A_133/2024**. Im Strafprozess lässt das Bundesgericht von Privaten rechtswidrig erlangte Beweise nur zu, wenn sie von den Behörden rechtmässig hätten erlangt werden können und eine Interessenabwägung für die Verwertung spricht **6B_768/2022**; Dashcam-Aufnahmen von Verkehrsregelverletzungen, die keine schweren Straftaten sind, blieben deshalb unverwertbar **BGE 146 IV 226**. Materielle Rechtfertigungsgründe des Datenschutzrechts ändern an der strafprozessualen Rechtswidrigkeit nichts, weil bei der Verwertbarkeit der Strafanspruch des Staates und das faire Verfahren im Vordergrund stehen **BGE 146 IV 226**.

Im Arbeitsrecht führte die Unverwertbarkeit zu materiellen Folgen: Die verdeckte Spyware-Überwachung blieb unverwertbar, sodass der fristlosen Kündigung die Grundlage fehlte **BGE 139 II 7**, und GPS-Daten aus einem privat nutzbaren Dienstwagen durften einem Lohnabzug nicht zugrunde gelegt werden **AH180153-L**. Dass die Abwägung auch zugunsten der Verwertung ausfallen kann, zeigt ein Entscheid des Bundesverwaltungsgerichts: Eine personenbezogene Auswertung von Internet-Protokolldaten war verfahrenswidrig, weil der Arbeitnehmer nicht vorgängig schriftlich über den konkreten Verdacht informiert worden war, blieb aber verwertbar, weil der Eingriff auf Protokolldaten beschränkt war und der Arbeitgeber mit Reglement und Warnhinweisen auf das Verbot aufmerksam gemacht hatte **a-6453-2014**.

Hinweise für die Praxis

- Zweck vor der Beschaffung festlegen und kommunizieren. Nachträgliche Information heilt fehlende Erkennbarkeit nicht **a-3891-2025**; Hinweise müssen konkret und vor der Erfassung wahrnehmbar sein, bei Kameras vor dem Betreten des Erfassungsbereichs **6B_768/2022**.
- Mildere Mittel dokumentieren. Gerichte prüfen regelmässig, ob Logfiles, technische Sperren, Verschlüsse oder Rechtsbehelfe des Schuldbetreibungsrechts genügt hätten **BGE 139 II 7 a-3891-2025 CACI pp20-043408-542/2022**.
- Aufbewahrungsfristen festlegen und mit gesetzlichen Aufbewahrungspflichten abstimmen **BBl 2017 6941 Art. 958f OR**.
- Richtigkeit risikogerecht kontrollieren und die getroffenen Massnahmen beweisbar festhalten, da der Bearbeiter sie nachweisen muss **ACJC/805/2025 a-4232-2015**.
- Einwilligungen eng und konkret fassen, Alternativen ohne unzumutbare Nachteile anbieten, in Abhängigkeitsverhältnissen einen anderen Rechtfertigungsgrund prüfen und für Abs. 7 eine aktive Erklärung einholen **a-2941-2024 a-3908-2008 150006614**.
- Beweisrisiko einkalkulieren. Grundsatzwidrig erhobene Daten können im Prozess unverwertbar sein und damit Kündigungen oder Forderungen ihre Grundlage entziehen **BGE 139 II 7 4A_133/2024**.