Art. 7 DSG: Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Funktion, Herkunft und Systematik

Art. 7 DSG verpflichtet den Verantwortlichen, den Datenschutz in die Bearbeitung selbst einzubauen, statt ihn erst nachträglich zu prüfen. Abs. 1 verlangt eine technische und organisatorische Ausgestaltung, welche die Einhaltung der Datenschutzvorschriften sicherstellt, und zwar ab der Planung ("Privacy by Design"). Abs. 2 legt den Angemessenheitsmassstab fest. Abs. 3 verlangt datenschutzfreundliche Voreinstellungen ("Privacy by Default").

Die Pflicht ist eine Neuerung der Totalrevision. Nach der Botschaft führt Art. 6 E-DSG die Pflicht zum Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen ein. Wegen ihres engen Zusammenhangs mit den Datenschutzgrundsätzen wurde sie in die allgemeinen Bestimmungen aufgenommen **BBl 2017 6941**. Für Bundesorgane war der Planungsgedanke nicht völlig neu. Sie mussten schon unter altem Recht Projekte zur automatisierten Bearbeitung melden, "damit die Erfordernisse des Datenschutzes bereits bei der Planung berücksichtigt werden" **BBl 2017 6941**.

Die Norm setzt nach der Botschaft das modernisierte Übereinkommen SEV 108 und Art. 20 Abs. 1 der Richtlinie (EU) 2016/680 um **BBl 2017 6941**. Das Übereinkommen verlangt die Anwendung der Grundsätze "unter Berücksichtigung der Art der Verarbeitung und gegebenenfalls der Grösse des Verantwortlichen" **BBl 2020 565**. Die Grösse des Verantwortlichen nennt der Schweizer Wortlaut nicht. Sie kann aber über "Art und Umfang der Datenbearbeitung" in die Angemessenheitsprüfung einfliessen.

Der Schlusstext stimmt mit der geltenden Fassung überein **BBl 2020 7639**. Seit dem Inkrafttreten am 1. September 2023 ist die Bestimmung unverändert. Im Parlament war sie unbestritten: Der Ständerat stimmte den Art. 6 bis 8 des Entwurfs ohne Diskussion im Sinne des Nationalrates zu **AB 2019 S 1240**.

Nach der Botschaft bringt die Norm den risikobasierten Ansatz zum Ausdruck **BBl 2017 6941**. Art. 7 DSG schreibt daher kein bestimmtes technisches Ergebnis vor. Verlangt ist eine Organisation der Bearbeitung, die dem Risiko angemessen ist. Die Bestimmung verbindet die materiellen Grundsätze (Art. 6 DSG) mit der Datensicherheit (Art. 8 DSG) und der Datenschutz-Folgenabschätzung (Art. 22 DSG).

Zeitlicher und persönlicher Anwendungsbereich

Laufende Bearbeitungen (Art. 69 DSG)

Art. 69 DSG nimmt bestimmte Bearbeitungen von Art. 7 aus, ebenso von den Art. 22 und 23. Die Bestimmung gilt nicht für Datenbearbeitungen, "die vor Inkrafttreten dieses Gesetzes begonnen wurden, wenn der Bearbeitungszweck unverändert bleibt und keine neuen Daten beschafft werden" **Art. 69 DSG**. Beide Voraussetzungen müssen erfüllt sein. Eine Zweckänderung lässt die Ausnahme entfallen, ebenso jede neue Datenbeschaffung, etwa die Erfassung neuer Kunden in einem bestehenden System. Von da an ist Art. 7 DSG voll zu beachten. Bei Systemen mit laufendem Datenzufluss hat die Ausnahme deshalb wenig praktische Tragweite.

Davon zu trennen ist Art. 70 DSG für hängige Untersuchungen. Im Fall Xplain beurteilte der EDÖB den Sachverhalt gestützt darauf nach altem Recht. Er hielt aber fest, dass das neue DSG zu keinem anderen Ergebnis führen würde und dass die Pflichten zur Datensicherheit durch die Prinzipien "Privacy by Design" und "Privacy by Default" (Art. 7 DSG) verstärkt werden **EDÖB Schlussbericht und Empfehlungen vom 25. April 2024 des Eidgenös** .

Das kantonale Recht kann einen anderen Massstab verwenden. Art. 58 KDSG/BE nimmt laufende Bearbeitungen von der Parallelnorm aus, wenn die Behörde ihre Pflichten nach altem Recht erfüllt hat und "sich die Bearbeitung nicht wesentlich ändert" **Art. 58 KDSG**. Entscheidend ist dort also, ob die Bearbeitung wesentlich geändert wird. Das Bundesrecht stellt dagegen auf eine Zweckänderung oder eine neue Datenbeschaffung ab.

Adressat: der Verantwortliche

Art. 7 DSG verpflichtet nur den Verantwortlichen. Das ist die private Person oder das Bundesorgan, die oder das allein oder zusammen mit anderen über Zweck und Mittel der Bearbeitung entscheidet **Art. 5 DSG**. Das passt zum Inhalt der Pflicht: Wer über die Mittel entscheidet, bestimmt auch Systemarchitektur und Voreinstellungen. Der TOM-Leitfaden des EDÖB hält entsprechend fest: "Für die Umsetzung solcher Massnahmen ist der Verantwortliche zuständig." **EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen**

Der Auftragsbearbeiter ist nur mittelbar gebunden. Der Unterschied zu Art. 8 DSG ist deutlich: Dort werden Verantwortlicher und Auftragsbearbeiter ausdrücklich gemeinsam verpflichtet **Art. 8 DSG**. Die Bindung des Auftragsbearbeiters an Art. 7 ergibt sich aus Art. 9 DSG. Danach dürfen die Daten nur so bearbeitet werden, "wie der Verantwortliche selbst es tun dürfte" **Art. 9 DSG**. Der Verantwortliche muss deshalb die Vorgaben nach Art. 7 vertraglich und technisch an den Auftragsbearbeiter weitergeben. Seine eigene Verantwortung bleibt bestehen: Nach dem Erläuternden Bericht zur DSV bleibt auch ein Verantwortlicher, der die Bearbeitung einem Auftragsbearbeiter überträgt, für den Datenschutz verantwortlich **EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) -** . Der gleiche Bericht spricht in seiner Gesamtübersicht davon, dass auch der Auftragsbearbeiter zu Privacy by Design und by Default verpflichtet sei **EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) -** . Diese Formulierung findet im Wortlaut von Art. 7 DSG keine Stütze. Massgebend bleibt der Gesetzestext.

Hersteller von Systemen und Software sind nicht Adressaten. Sie können ihre Produkte jedoch freiwillig zertifizieren lassen (Art. 13 Abs. 1 DSG) **Art. 13 DSG**. Praktisch wirkt die Pflicht des Verantwortlichen auf die Hersteller zurück. Der EDÖB erwartet, dass private Verantwortliche vor dem Einsatz von Überwachungsprodukten wie Smartglasses prüfen, ob Hersteller und Anbieter "die Vorgabe einer datenschutzfreundlichen Ausgestaltung und Konfiguration ihrer Überwachungsprodukte i. S. v. Art. 7 DSG umsetzen." **EDÖB 33. Tätigkeitsbericht 2025/2026** Bei Bundesorganen verlagert sich die Pflicht damit in die öffentliche Beschaffung. Im Vordergrund stehen Anforderungen an die Konfigurierbarkeit von Programmen, mit

denen das Bundesorgan die technisch mögliche Intensität der Bearbeitung auf das Mass senken kann, das mit seinen gesetzlichen Aufgaben vereinbar ist **EDÖB 33. Tätigkeitsbericht 2025/2026**

Das DSG gilt für private Personen und Bundesorgane **Art. 2 DSG**. Kantonale und kommunale Organe unterstehen Art. 7 DSG nicht. Für sie gelten die kantonalen Parallelnormen (dazu unten).

Datenschutz durch Technik (Abs. 1)

Gegenstand: alle Datenschutzvorschriften, besonders Art. 6 DSG

Art. 7 Abs. 1 DSG verlangt eine Ausgestaltung, welche die Einhaltung "der Datenschutzvorschriften" sicherstellt. Die Grundsätze nach Art. 6 DSG nennt die Bestimmung nur "insbesondere". Der Bezugspunkt ist deshalb weiter als Art. 6 und umfasst etwa auch die Betroffenenrechte. Der Erläuternde Bericht zur DSV verbindet "Privacy by Design" ausdrücklich mit dem Auskunftsrecht: Verantwortliche müssen über ein System verfügen, das einen einfachen Zugang zu den bearbeiteten Daten ermöglicht **EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) - Erläuternder Bericht** .

Im Kern geht es darum, die Grundsätze des Art. 6 DSG technisch umzusetzen: Verhältnismässigkeit, Zweckbindung und Erkennbarkeit, Vernichtung oder Anonymisierung nicht mehr erforderlicher Daten sowie Richtigkeit **Art. 6 DSG**. Die Botschaft nennt als Beispiele, dass Daten "in regelmässigen Abständen gelöscht oder standardmässig anonymisiert" werden **BBl 2017 6941**. Der TOM-Leitfaden des EDÖB führt weitere Massnahmen auf, darunter Pseudonymisierung, Verschlüsselung und Minimierung. Er hält fest, dass eine vollständige Löschung "wesentlich einfacher zu bewerkstelligen" ist, wenn das System nach den Grundsätzen des Datenschutzes durch Technik konzipiert wurde **EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM)** .

Zu den organisatorischen Massnahmen gehören nach der Praxis des EDÖB Löschkonzepte, die Sensibilisierung und Schulung der Mitarbeitenden sowie periodische interne oder externe Audits **EDÖB 32. Tätigkeitsbericht 2024/2025** Der Fall Xplain zeigt die praktische Bedeutung. Ein Softwarelieferant der Bundesverwaltung hatte Personendaten nach der Fehlerbehebung im Support weiter aufbewahrt. Der EDÖB hielt fest, dass nach Erfüllung des Zwecks die Daten "vorbehältlich einer Aufbewahrungspflicht" zu löschen sind, und empfahl die Umsetzung eines Löschkonzepts **EDÖB Schlussbericht und Empfehlungen vom 25. April 2024 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in Sach** . Der Bericht beruht auf altem Recht (siehe oben) und zeigt deshalb nur mittelbar, was Art. 7 DSG verlangt.

Ein Beispiel für eine Gestaltung, die gegen die Grundsätze verstösst, ist der Fall Digitec Galaxus. Für eine Bestellung musste zwingend ein Kundenkonto eröffnet werden, obwohl die daraus folgenden Bearbeitungen für die Abwicklung des Kaufvertrags nicht notwendig waren. Diese Koppelung beurteilte der EDÖB als Verstoss gegen das Verhältnismässigkeitsprinzip **EDÖB 32. Tätigkeitsbericht 2024/2025** Der EDÖB stützte sich dabei auf Art. 6 DSG und nicht ausdrücklich auf Art. 7. Der Fall zeigt aber, dass die Gestaltung des Bestellprozesses selbst Gegenstand der datenschutzrechtlichen Prüfung ist.

Zeitpunkt: ab der Planung und während des ganzen Lebenszyklus

Nach Abs. 1 Satz 2 muss der Verantwortliche die Anforderungen "ab der Planung" berücksichtigen. Der TOM-Leitfaden fasst das so: Die Grundsätze sind ab der Planung des Systems mitzuberücksichtigen, "und nicht erst später" **EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM)** . Mit der Planung endet die Pflicht aber nicht. Die Massnahmen sind nach dem Leitfaden "während des ganzen Lebenszyklus" der Daten zu implementieren und müssen auf jeder Stufe des Systems greifen **EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen** . Für die Datensicherheit verlangt Art. 1 Abs. 5 DSV ausdrücklich, Schutzbedarf, Risiko und Massnahmen über die gesamte Bearbeitungsdauer zu überprüfen und nötigenfalls anzupassen **Art. 1 DSV**. Diese Regel betrifft unmittelbar nur Art. 8 DSG. Sie lässt sich aber auf Art. 7 übertragen, weil auch dessen Massstab dynamisch ist ("Stand der Technik").

In der Aufsichtspraxis über Bundesprojekte setzt der EDÖB früh an. Für einen neuen Personenidentifikator im Gesundheitswesen (DigiSanté) verlangte er ein Konzept "des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen im Sinne von Art. 7 DSG sowie eine Datenschutz-Folgenabschätzung nach Art. 22 DSG", wenn neue Projekte oder Entwicklungen geplant werden **EDÖB 31. Tätigkeitsbericht 2023/2024** Bei der E-ID soll der Datenschutz "durch das System selber" gewährleistet werden **EDÖB 31. Tätigkeitsbericht 2023/2024** Der EDÖB trat dort zudem für den Grundsatz der Nicht-Nachverfolgbarkeit ein und verlangte, den Zugriff auf nicht erforderliche Daten zu verhindern **EDÖB 32. Tätigkeitsbericht 2024/2025** Bei Überwachungsanlagen von Bundesorganen besteht nach dem EDÖB schon "im frühen Stadium der öffentlichen Beschaffung" Bedarf für eine erste Risikoevaluation **EDÖB 33. Tätigkeitsbericht 2025/2026**

Angemessenheit der Massnahmen (Abs. 2)

Die Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Bearbeitung sowie dem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen angemessen sein. Nach der Botschaft sind beim Risiko die "Eintrittswahrscheinlichkeit und Schwere" massgebend **BBl 2017 6941**. Die Aufzählung ist nicht abschliessend ("insbesondere"). Daraus folgt eine gleitende Skala: Je sensibler die Daten, je umfangreicher die Bearbeitung und je höher das Risiko, desto weiter gehen die geschuldeten Vorkehren. Art. 6 Abs. 5 DSG verwendet für die Massnahmen zur Richtigkeit eine nahezu gleichlautende Angemessenheitsformel **Art. 6 DSG**. Das spricht dafür, beide Formeln einheitlich auszulegen.

Kosten nennt Art. 7 Abs. 2 DSG nicht. Ausdrücklich erwähnt werden die "Implementierungskosten" nur in Art. 1 Abs. 4 lit. b DSV, und zwar für die Datensicherheit **Art. 1 DSV**. Der Erläuternde Bericht versteht die Kosten dort weit, als finanzielle, personelle und zeitliche Ressourcen. Er hält zugleich fest, dass sich Verantwortliche "nicht mit der Begründung von der Pflicht einer angemessenen Datensicherheit befreien" können, dass damit übermässige Kosten verbunden sind **EDÖB Verordnung über den Datenschutz (Datenschutzverordnung, DSV) -** . Für Art. 7 DSG ist es naheliegend, Kosten im Rahmen der Angemessenheit zu berücksichtigen. Ein Kostenargument kann aber auch hier keine Bearbeitung rechtfertigen, die gegen die Grundsätze verstösst. Bei der Datensicherheit ist das ausdrücklich so geregelt. Für Art. 7 ergibt es sich daraus, dass Abs. 1 die Einhaltung der Datenschutzvorschriften als Ergebnis verlangt.

Wie der risikobasierte Massstab gerichtlich angewendet wird, zeigt ein Entscheid des Obergerichts Zürich vom 8. Januar 2026 zur Datensicherheit. Das Gericht verneinte eine Pflicht zur Ende-zu-Ende-Verschlüsselung beim Versand von Rechnungs- und Adressdaten. Es hielt fest: "Stattdessen gilt ein risikobasierter Ansatz: Unternehmen müssen geeignete Massnahmen auf Basis einer Risikoanalyse wählen." **UE240472** Der Entscheid betrifft Art. 8 DSG und ist für Art. 7 Abs. 2 nur sinngemäss heranzuziehen. Er zeigt aber, dass weder DSG noch DSV eine bestimmte Technik vorschreiben und dass die Einstufung der Daten das geschuldete Schutzniveau massgeblich bestimmt.

Der "Stand der Technik" ist ein dynamischer Massstab. Ein Urteil des Bundesverwaltungsgerichts zur Funk- und Kabelaufklärung zeigt die Kontrollintensität des Datenschutzes im eingriffsintensiven Bereich, allerdings im Rahmen der Grundrechtsprüfung und nicht gestützt auf Art. 7 DSG. Das Gericht übernahm die Anforderung, den Dienst zu verpflichten, "die Filtermethoden kontinuierlich fortzuentwickeln und

auf dem Stand von Wissenschaft und Technik zu halten" **a-6444-2020** . Ein einmal konformes System kann deshalb mit fortschreitender Technik ungenügend werden.

Datenschutzfreundliche Voreinstellungen (Abs. 3)

Inhalt: Mindestmass als Ausgangszustand

Abs. 3 verlangt, dass die Bearbeitung durch geeignete Voreinstellungen auf das für den Verwendungszweck nötige Mindestmass beschränkt ist. Nach der Botschaft sollen "grundsätzlich nur so wenige Personendaten bearbeitet werden, wie im Hinblick auf den Verwendungszweck möglich ist" **BBl 2017 6941**. Der TOM-Leitfaden bezeichnet die Voreinstellungen als "Ausdruck des Grundsatzes der Verhältnismässigkeit" **EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM)** . Abs. 3 bezieht sich auf den Ausgangszustand eines Systems, also auf das, was ohne Zutun der betroffenen Person geschieht. Die Bestimmung ist deshalb besonders bei Massendiensten wie Websites, Apps und Kundenkonten wichtig. Als einfache Massnahme nennt der Leitfaden, für nicht notwendige Datenfelder einen Wert vorzusehen, "der auf null oder negativ voreingestellt ist (z. B. «NA»)" **EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM)** .

Vorbehalt der Bestimmung durch die betroffene Person

Die Voreinstellung gilt, "soweit die betroffene Person nicht etwas anderes bestimmt". Abs. 3 verbietet also eine weitergehende Bearbeitung nicht. Die Bestimmung legt fest, wer die Abweichung vom Minimum veranlassen muss: die betroffene Person, nicht der Verantwortliche. Ob für die weitergehende Bearbeitung eine Einwilligung nötig ist, ergibt sich nicht aus Art. 7. Massgebend sind die allgemeinen Regeln. Ist eine Einwilligung erforderlich, so muss sie nach Art. 6 Abs. 6 DSG für bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt werden. Bei besonders schützenswerten Daten und bei Profiling mit hohem Risiko durch Private muss sie zudem ausdrücklich erfolgen (Art. 6 Abs. 7 DSG) **Art. 6 DSG**.

Der Cookie-Leitfaden des EDÖB zeigt, wie Art. 7 Abs. 3 und die Einwilligungsregeln zusammenwirken:

- Der Webseitenbetreiber muss durch Voreinstellungen sicherstellen, dass der Cookie-Einsatz auf das nötige Mindestmass beschränkt bleibt. Das gilt, bis die Besucherin oder der Besucher die Bearbeitung tatsächlich zur Kenntnis nehmen und widersprechen kann **EDÖB Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien** .
- Stützt sich eine Bearbeitung durch Dritte auf eine Einwilligung, darf sie nicht schon beim Aufruf der Webseite standardmässig aktiviert sein. Empfohlen wird eine Zwei-Klick-Lösung **EDÖB Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien** .
- Verlangt das Gesetz keine ausdrückliche Einwilligung, sind vorangekreuzte Kästchen nicht ausgeschlossen. Die Abwahl darf aber nicht komplizierter gestaltet sein als die Auswahl **EDÖB Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien** .

Der TOM-Leitfaden formuliert strenger: Nicht notwendige Cookies "sollten" standardmässig deaktiviert sein, sodass Nutzende der Verwendung zusätzlicher Cookies "aktiv zustimmen müssen" **EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM)** . Die beiden Dokumente lassen sich vereinbaren. Der Cookie-Leitfaden ist die speziellere Stellungnahme und knüpft die Opt-in-Pflicht an die Frage, ob eine Einwilligung rechtlich erforderlich ist. Beide Leitfäden sind Verwaltungspraxis und für die Gerichte nicht verbindlich.

Wie der EDÖB den Vorbehalt durchsetzt, zeigt erneut der Fall Digitec Galaxus. Die zuvor beanstandete übermässige Datenbearbeitung kann seither durch eine einmalige Handlung deaktiviert werden ("One-click-opt-out"), weil die Personalisierung der Website neu mit einem Klick ausgeschaltet werden kann **EDÖB 33. Tätigkeitsbericht 2025/2026** Der Fall zeigt, worauf es ankommt: Die betroffene Person muss ihre Bestimmungsbefugnis tatsächlich und ohne unverhältnismässigen Aufwand ausüben können.

Abgrenzung zur Datensicherheit (Art. 8 DSG)

Nach der Botschaft stehen Datenschutz und Datensicherheit "zwar in einer Wechselwirkung, sind aber voneinander abzugrenzen". Beim Datenschutz geht es um den Persönlichkeitsschutz des Einzelnen. Die Datensicherheit zielt dagegen generell auf die vorhandenen Daten und "umfasst den allgemeinen technischen und organisatorischen Rahmen der Datenbearbeitung" **BBl 2017 6941**. Art. 7 DSG fragt deshalb, ob das System rechtmässig, verhältnismässig und zweckgebunden bearbeitet. Art. 8 DSG fragt, ob die Daten vor Verlust, unbefugtem Zugriff und Veränderung geschützt sind **Art. 8 DSG**.

Drei Unterschiede sind praktisch wichtig. Erstens verpflichtet Art. 8 DSG auch den Auftragsbearbeiter **Art. 8 DSG**. Zweitens ist nur Art. 8 durch Verordnungsrecht konkretisiert: Art. 1 bis 3 DSV regeln Schutzbedarf, Risikobeurteilung und einen Katalog von Kontrollzielen, etwa Zugriffs-, Speicher- und Eingabekontrolle **Art. 1 DSV Art. 3 DSV** . Zu Art. 7 DSG enthält die DSV keine eigenen Ausführungsbestimmungen. Drittens ist nur die Missachtung der Mindestanforderungen nach Art. 8 Abs. 3 DSG strafbar (dazu unten).

Die Bereiche überschneiden sich in der Zugriffssteuerung. Nach Art. 3 Abs. 1 lit. a DSV dürfen berechtigte Personen nur auf jene Daten zugreifen, die sie zur Erfüllung ihrer Aufgaben benötigen **Art. 3 DSV**. Ein Berechtigungskonzept nach diesem Grundsatz dient der Sicherheit und zugleich der Verhältnismässigkeit. Ein Genfer Strafentscheid zeigt die Abgrenzung. Gerügt war, dass das Abrechnungspersonal einer Arztpraxis vollen Zugriff auf die Patientendossiers hatte und dies Art. 7 Abs. 1 DSG verletze. Die Software erlaubte keinen Teilzugriff. Die Chambre pénale de recours beurteilte den Vorwurf nur unter Art. 61 lit. c in Verbindung mit Art. 8 DSG. Die Frage der Verhältnismässigkeit des Zugriffs "relève essentiellement du droit civil" (sie gehört im Wesentlichen ins Zivilrecht) **ACPR/239/2025**. Mängel in der Zugriffsgestaltung sind somit vor allem ein Problem von Art. 6 und 7 DSG und nur ausnahmsweise ein strafrechtliches.

Nachweis und Dokumentation: DSFA, Zertifizierung, Verhaltenskodizes

Art. 7 DSG enthält keine eigene Dokumentationspflicht. Nach der Botschaft kann der Verantwortliche "insbesondere durch die Zertifizierung oder eine Datenschutz-Folgenabschätzung aufzeigen", dass er der Bestimmung nachkommt **BBl 2017 6941**. Bei hohem Risiko ist eine DSFA ohnehin vorgängig zu erstellen. Sie muss die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte enthalten **Art. 22 DSG**. Der TOM-Leitfaden hält fest, dass die Massnahmen nach Art. 7 "in der Regel in einer DSFA detailliert beschrieben" werden **EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen** . Die DSFA ist damit das Planungsinstrument, in dem Art. 7 Abs. 1 Satz 2 praktisch umgesetzt wird.

Zertifizierte Systeme, Produkte und Dienstleistungen (Art. 13 DSG) und Verhaltenskodizes (Art. 11 DSG) können den Nachweis erleichtern **Art. 13 DSG Art. 11 DSG**. Ein privater Verantwortlicher kann unter den Voraussetzungen von Art. 22 Abs. 5 DSG sogar auf eine DSFA verzichten **Art. 22 DSG**. Das Verzeichnis der Bearbeitungstätigkeiten erfasst dagegen nur die Massnahmen zur Datensicherheit nach Art. 8, und zwar "wenn möglich" **Art. 12 DSG**. Wer Art. 7 DSG belegen will, muss diese Lücke durch eine eigene

Dokumentation schliessen. Nach dem EDÖB müssen Bundesorgane und private Unternehmen nach der Risikoanalyse ihre Umsetzungsprozesse "wie Datenflüsse, Anonymisierung oder Zugriffsmodalitäten" vollständig und verständlich dokumentieren **EDÖB 32. Tätigkeitsbericht 2024/2025**

Rechtsfolgen einer Verletzung

Aufsichtsrechtliche Durchsetzung

Am direktesten wird Art. 7 DSG aufsichtsrechtlich durchgesetzt. Der EDÖB eröffnet eine Untersuchung, wenn genügend Anzeichen für einen Verstoss bestehen. Bei Verletzungen von geringfügiger Bedeutung kann er darauf verzichten **Art. 49 DSG**. Er kann namentlich anordnen, dass das Bundesorgan oder die private Person "die Vorkehren nach den Artikeln 7 und 8 trifft". Stellt der Betroffene die Einhaltung während der Untersuchung wieder her, kann sich der EDÖB auf eine Verwarnung beschränken **Art. 51 DSG**. Die Massnahmen ergehen als Verfügung nach VwVG. Partei ist nur, wer untersucht wird **Art. 52 DSG**. Beschwerdeinstanz ist das Bundesverwaltungsgericht **EDÖB Untersuchung von Verstössen gegen Datenschutzvorschriften durch den EDÖB (Analyse Art. 49ff)**. Verwaltungssanktionen gegen Unternehmen sah der Bundesrat bewusst nicht vor **BBl 2017 6941**.

Das Bundesverwaltungsgericht hat betont, dass der Verantwortliche die Einhaltung der Datenschutzvorschriften nicht davon abhängig machen kann, ob der EDÖB ihn auf eine Verletzung aufmerksam macht. Vielmehr "obliegt es der Beschwerdeführerin selbst, dafür zu sorgen, dass die Datenschutzvorschriften eingehalten werden" **a-3891-2025**. Der Entscheid betraf eine Verletzung von Art. 6 DSG, nicht von Art. 7. Er bestätigt aber die präventive Ausrichtung des Gesetzes, auf der Art. 7 beruht.

Zivilrechtliche Ansprüche und Ansprüche gegenüber Bundesorganen

Art. 30 Abs. 2 lit. a DSG nennt als Persönlichkeitsverletzung die Bearbeitung entgegen den Grundsätzen nach Art. 6 und 8 DSG. Art. 7 ist dort nicht genannt **Art. 30 DSG**. Die Aufzählung ist nicht abschliessend ("insbesondere"). Eine fehlerhafte Systemgestaltung wird aber in der Regel nur mittelbar Klagen nach Art. 32 DSG und Art. 28 ff. ZGB begründen: dann, wenn sie zu einer unverhältnismässigen, zweckwidrigen oder unsicheren Bearbeitung führt **Art. 32 DSG**. Die betroffene Person muss deshalb die Folge der Gestaltung (etwa eine übermässige Datenerhebung) nachweisen, nicht bloss den Gestaltungsmangel. Gegenüber Bundesorganen gilt dasselbe für die Ansprüche auf Unterlassung, Beseitigung und Feststellung einer widerrechtlichen Bearbeitung nach Art. 41 DSG **Art. 41 DSG**.

Keine Strafbarkeit

Art. 7 DSG ist nicht strafbewehrt. Art. 61 DSG erfasst unter den Sorgfaltspflichten nur die Bekanntgabe ins Ausland, die Übertragung an Auftragsbearbeiter und in lit. c die vorsätzliche Missachtung der Mindestanforderungen an die Datensicherheit nach Art. 8 Abs. 3 DSG **Art. 61 DSG**. Die kantonale Praxis legt sogar lit. c eng aus. Nach der Genfer Chambre pénale de recours fallen nur schwere oder offensichtliche Fälle darunter: "l'absence complète de mesures de sécurité serait certainement punissable" (das völlige Fehlen von Sicherheitsmassnahmen wäre sicher strafbar), ungenügende Massnahmen dagegen grundsätzlich nicht **ACPR/239/2025**. Das Obergericht Zürich bestätigte ebenfalls eine Nichtanhandnahme, weil kein vorsätzlicher Verstoss ersichtlich war **UE240472**. Wer eine Strafanzeige auf Art. 7 DSG stützt, wird daher in aller Regel scheitern. Der geeignete Weg ist die Anzeige beim EDÖB oder eine Zivilklage.

Typische Anwendungsfelder

Zugriffskonzepte in Informationssystemen. Die Genfer Chambre administrative beurteilte nach kantonalem Recht (Art. 37 LIPAD) das Zugriffssystem eines Spitals auf elektronische Patientendossiers **ATA/663/2024** Der Zugriff hing von drei Faktoren ab: dem Profil, dem Tätigkeitsbereich und einem zeitlichen Bezug zur Behandlung. Für Notfälle bestand ein Ausnahmezugriff ("vitre brisée"). Dieser war bestimmten Profilen vorbehalten, verlangte eine Begründung und wurde protokolliert. Das Gericht hielt fest: "L'ensemble des accès est ainsi journalisé, ce qui permet un contrôle a posteriori des éventuels abus" (alle Zugriffe werden so protokolliert, was eine nachträgliche Kontrolle allfälliger Missbräuche erlaubt) **ATA/663/2024** Das System als Ganzes war rechtmässig. Rechtswidrig war dagegen der Einzelzugriff einer Ärztin ausserhalb jeder Behandlungsbeziehung: Sie hatte die Schutzmassnahmen umgangen, indem sie fälschlich angab, den Patienten zu behandeln. Der Entscheid beruht auf kantonalem Recht und lässt sich auf Art. 7 DSG nur sinngemäss übertragen. Er zeigt aber, was angemessene Vorkehren leisten: Sie müssen Missbräuche nicht vollständig ausschliessen, aber eingrenzen und nachvollziehbar machen. Ähnlich verlangte der EDÖB nach einem unrechtmässigen Zugriff auf das SIS beim Grenzwachtkorps Anpassungen im Berechtigungsmanagement und Eigenkontrollen **EDÖB 32. Tätigkeitsbericht 2024/2025**

Videoüberwachung. Am Arbeitsplatz sind Kameras so zu positionieren und einzustellen, "dass der Aufnahmebereich auf ein Minimum begrenzt ist" und die Angestellten eine Rückzugsmöglichkeit haben **EDÖB 32. Tätigkeitsbericht 2024/2025** Aufzeichnungen sind nach Erfüllung des Zwecks unverzüglich zu löschen **EDÖB 33. Tätigkeitsbericht 2025/2026** Das ist eine typische Anwendung von Abs. 1 und 3: Ausrichtung, Ausschnitt und Speicherdauer werden technisch festgelegt.

Staatliche Datensysteme. Für die öffentliche Hand verbindet sich der Gedanke von Art. 7 mit verfassungsrechtlichen Anforderungen. In BGE 151 I 137 verlangte das Bundesgericht gestützt auf Art. 13 BV für polizeiliche Systeme zur Fahrzeugfahndung und zum Datenaustausch "organisatorischer, technischer und verfahrensrechtlicher Schutzvorkehrungen, soweit sich diese nicht bereits aus der Datenschutzgesetzgebung oder anderen Bestimmungen ergeben" **BGE 151 I 137**. Es hob Luzerner Bestimmungen auf, weil unter anderem Regeln zur Protokollierung und zur unabhängigen Kontrolle fehlten **BGE 151 I 137**. Das Urteil betrifft kantonales Polizeirecht und nicht Art. 7 DSG. Es zeigt aber, dass bei schweren Grundrechtseingriffen ein Teil der technischen Ausgestaltung schon im Gesetz selbst festgelegt sein muss.

Kantonale Parallelnormen

Für kantonale Organe haben mehrere Kantone eigene Bestimmungen erlassen. Diese weichen im Detail voneinander ab:

- Bern: Art. 9 KDSG/BE übernimmt die Bundesnorm weitgehend wörtlich, samt "ab der Planung" und dem Vorbehalt der Bestimmung durch die betroffene Person. Beim Risiko stellt er auf das "Risiko für die betroffenen Personen" ab **Art. 9 KDSG**. Für laufende Bearbeitungen gilt die eigene Übergangsregel (siehe oben).
- Zug: Art. 7a DSG/ZG verpflichtet die "Organe". Er enthält weder den Planungssatz noch den Hinweis auf die Grundsätze und bezieht das Risiko nur auf die Grundrechte **Art. 7a DSG/ZG**.
- Basel-Stadt: § 14 IDG/BS verlangt Massnahmen "von Anfang an", um Grundrechtsverletzungen vorzubeugen. Er enthält keinen Katalog von Angemessenheitskriterien. Die Voreinstellungen müssen sicherstellen, dass "standardmässig" nur die erforderlichen Daten bearbeitet werden, ohne Vorbehalt einer abweichenden Bestimmung durch die betroffene Person **Art. 14 Informations- und Datenschutzgesetz, IDG**.
- Genf: Die Chambre administrative beurteilte das Zugriffssystem eines Spitals nach Art. 37 LIPAD **ATA/663/2024** (dazu oben, Typische Anwendungsfelder).

Bei Bearbeitungen durch kantonale Behörden ist deshalb stets die einschlägige kantonale Norm zu prüfen. Die Bundespraxis kann dafür

höchstens als Auslegungshilfe dienen.

Hinweise für die Praxis

- Übergang prüfen: Klären Sie, ob eine vor dem 1. September 2023 begonnene Bearbeitung unter Art. 69 DSG fällt. Mit jeder Zweckänderung oder neuen Datenbeschaffung entfällt die Ausnahme.
- Früh ansetzen: Datenschutzanforderungen gehören in Pflichtenhefte, Beschaffungsunterlagen und Verträge mit Auftragsbearbeitern.
- Voreinstellungen testen: Prüfen Sie, welche Daten ohne Zutun der Nutzenden bearbeitet werden. Beim Einsatz nicht notwendiger Cookies und bei Personalisierung gilt: Eine Abwahl darf nicht schwieriger sein als eine Zustimmung.
- Dokumentieren: Halten Sie Risikobeurteilung, gewählte Massnahmen und Löschkonzept fest, bei hohem Risiko in der DSFA. Das Verzeichnis nach Art. 12 DSG genügt dafür nicht.
- Rechtsweg richtig wählen: Statt einer Strafanzeige kommen die Anzeige beim EDÖB oder eine Zivilklage gegen die konkrete Bearbeitungsfolge in Betracht (siehe oben, Rechtsfolgen einer Verletzung).