ONLINEKOMMENTAR
DER FREI ZUGÄNGLICHE
RECHTSKOMMENTAR

KOMMENTIERUNG ZU

Art. 6 Abs. 3-5 DSG

Eine Kommentierung von Caroline Gaul
Herausgegeben von Thomas Steiner / Anne-Sophie Morand / Daniel Hürlimann

Stand der Bearbeitung: 28.03.2025
PDF erstellt am: 06.10.2026
DOI: 10.17176/20250328-214043-0

ZITIERVORSCHLAG

Caroline Gaul, Kommentierung zu Art. 6 Abs. 3-5 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Kurzzitat: OK-Gaul, Art. 6 Abs. 3-5 DSG N. XXX.

Art. 6 Grundsätze

[...]

[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.

[4] Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.

[5] Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Massnahmen hängt namentlich ab von der Art und dem Umfang der Bearbeitung sowie vom Risiko, das die Bearbeitung für die Persönlichkeit oder Grundrechte der betroffenen Personen mit sich bringt.

GLIEDERUNG

In Kürze ... 3
I. Allgemeines ... 3
A. Vorbemerkungen ... 3
B. Hintergrund und Normzweck ... 4
C. Adressat der Pflichten ... 4
D. Rechtliche und wirtschaftliche Folgen einer Verletzung ... 5
E. Entstehungsgeschichte der einzelnen Bearbeitungsgrundsätze ... 5
1. Grundsatz der Zweckbindung und Transparenz, Art. 6 Abs. 3 DSG ... 5
2. Zeitliche Limitierung der Datenbearbeitung, Art. 6 Abs. 4 DSG ... 6
3. Grundsatz der Richtigkeit, Art. 6 Abs. 5 DSG ... 6
II. Gegenstand der Bestimmungen ... 6
A. Grundsatz der Zweckbindung und Transparenz, Art. 6 Abs. 3 DSG ... 6
1. Anforderungen ... 6
2. Beispiele ... 7
3. Empfehlungen zur Umsetzung ... 10
B. Zeitliche Limitierung der Datenbearbeitung, Art. 6 Abs. 4 DSG ... 11
1. Anforderungen ... 11
2. Empfehlungen zur Umsetzung ... 12
C. Grundsatz der Richtigkeit, Art. 6 Abs. 5 DSG ... 12
1. Richtigkeit der Daten ... 12
a. Anforderungen ... 12
b. Beispiele ... 14
2. Vergewisserungspflicht, Berichtigungs- und Löschungspflicht ... 15
a. Anforderungen ... 15
b. Beispiele ... 15
3. Empfehlungen zur Umsetzung ... 16
Literaturverzeichnis ... 17
Materialienverzeichnis ... 17

IN KÜRZE

Die Bestimmungen der Art. 6 Abs. 3 DSG (**Zweckbindung und Transparenz**), Art. 6 Abs. 4 DSG (**zeitliche Limitierung der Datenbearbeitung**) und Art. 6 Abs. 5 DSG (**Richtigkeit**) gehören zu den so genannten **Bearbeitungsgrundsätzen**, den wichtigsten materiellen Grundsätzen des Datenschutzrechts. Sie sind wesentlich für die konkrete Ausgestaltung der Datenbearbeitung.

Ein Verstoss gegen die Bearbeitungsgrundsätze stellt eine Verletzung der Persönlichkeitsrechte der Betroffenen dar. Die Persönlichkeitsverletzung kann bei privaten Datenbearbeitern aber durch Einwilligung, ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt sein. Dieser wesentliche Unterschied zur DSGVO der EU, bei der jede Datenbearbeitung einer konkreten rechtlichen Grundlage bedarf, wurde auch im neuen DSG aufrechterhalten.

Eine Verletzung der hier behandelten Bearbeitungsgrundsätze ist - ebenfalls anders als unter der DSGVO der EU - nach DSG nicht bussgeldbewehrt, kann aber weitreichende Folgen nach sich ziehen, insbesondere vor dem Hintergrund der mit dem neuen DSG erweiterten Befugnisse des Eidgenössischen Datenschutzbeauftragten (EDÖB). Dieser kann verfügen, dass die Datenbearbeitung ganz oder teilweise angepasst, unterbrochen oder sogar abgebrochen wird und die Personendaten ganz oder teilweise vernichtet werden. Darüber hinaus sollten mögliche (zivilrechtliche) Rechtsansprüche der Betroffenen und insbesondere auch die Folgen eines **Vertrauensverlusts** und **Reputationsschadens** berücksichtigt werden.

I. ALLGEMEINES

A. Vorbemerkungen

1 Die Bestimmungen der Art. 6 Abs. 3 DSG (**Zweckbindung und Transparenz**), Art. 6 Abs. 4 DSG (**zeitliche Limitierung der Datenbearbeitung**) und Art. 6 Abs. 5 DSG (**Richtigkeit**) gehören zusammen mit Art. 6 As. 1 DSG (Rechtmässigkeit), Art. 6 Abs. 2 (Verhältnismässigkeit und Treu und Glauben), und Art. 8 DSG (Datensicherheit) zu den so genannten **Bearbeitungsgrundsätzen**, den wichtigsten materiellen Grundsätzen des Datenschutzes und den eigentlichen Leitideen des Gesetzes.[1] Die Artikel 6 Abs. 6 und Abs. 7 DSG (Einwilligung) sind keine Bearbeitungsgrundsätze, sondern erläutern lediglich die Voraussetzungen der Einwilligung.[2]

2 Die Bearbeitungsgrundsätze des DSG gelten für private Datenbearbeiter ebenso wie für Organe des Bundes. Ein Verstoss gegen die Bearbeitungsgrundsätze stellt eine **Verletzung der Persönlichkeit** dar. Bei privaten Datenbearbeitern ist aber nicht jede Verletzung der Persönlichkeit widerrechtlich. Vielmehr kann sie durch Einwilligung der betroffenen Person, durch überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt sein (Art. 31 Abs. 1 DSG). Dieser wesentliche Unterschied zur DSGVO der EU, bei der jede Datenbearbeitung eines Rechtfertigungsgrundes bedarf (Verbot mit Erlaubnisborbehalt), wurde im Zuge der Revision des DSG aufrechterhalten. Damit wird nach Schweizer Datenschutzrecht bei privaten Datenbearbeitern auch weiterhin nur dann eine Rechtsgrundlage verlangt, wenn überhaupt eine Persönlichkeitsverletzung vorliegt.[3] Für die Datenbearbeitung durch Bundesbehörden gilt im Gegensatz zu der Bearbeitung durch Private auch

1. Botschaft DSG 1988, S. 433 und 449.
2. Botschaft DSG 2003, S. 2127; Botschaft DSG 2017, S. 6952; Gaspare T. Loderer, Kommentierung zu Art. 6 Abs. 6 und 7 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz, N. 5 – Version: 8.1.2024: https://onlinekommentar.ch/de/kommentare/art6abs6und7 (besucht am 6.5.2024), DOI: 10.17176/20240127-143131-0; OFK DSG Steiner/Laux, Art. 30 DSG N. 12.

nach Schweizer Datenschutzrecht, dass es grundsätzlich einer Rechtsgrundlage bedarf (Verbot mit Erlaubnisvorbehalt).[4] Auch wenn und soweit eine solche vorhanden ist, gelten grundsätzlich ebenfalls die Bearbeitungsgrundsätze.[5] Sie stellen unmittelbar anwendbares Verhaltensrecht dar, gegen dessen Verletzung die betroffene Person rechtlich vorgehen kann.[6] Ob und wieweit Bundesbehörden von der Einhaltung der Bearbeitungsgrundsätze ausnahmsweise befreit sind, muss anhand der gesetzlichen Grundlage bestimmt werden.[7]

3 Die Grundsätze der Datenbearbeitung gelten für den gesamten Lebenszyklus der Datenbearbeitung, unabhängig von den angewandten Mitteln und Verfahren und sind damit **technologieneutral**, d.h. ohne Bezugnahme auf konkrete technische oder kommerzielle Anwendungen ausgestaltet.[8]

B. Hintergrund und Normzweck

4 Der schweizerische Gesetzgeber betont von jeher, dass das Schweizer Datenschutzgesetz nicht den Zweck hat, die Entwicklungsmöglichkeiten im Bereich der Informationstechnologien zu verhindern oder einzuschränken.[9] Vielmehr soll in der Schweiz eine kohärente und **zukunftsorientierte Datenpolitik** entwickelt werden.[10] Der EDÖB hat in diesem Zusammenhang ausdrücklich festgehalten, dass auch unter dem neuen Datenschutzgesetz potenziell hohe Bearbeitungsrisiken kein Killerargument gegen Vorhaben der digitalen Transformation darstellen.[11] Gewisse **Leitplanken** sind aber einzuhalten. Dazu gehören, neben den weiteren Bearbeitungsgrundsätzen, der hier behandelte Grundsatz der Zweckbindung (Art. 6 Abs. 3 DSG), die Bestimmungen zur Dauer der Datenbearbeitung (Art. 6 Abs. 4 DSG) und die Anforderungen an die Richtigkeit der Daten (Art. 6 Abs. 5 DSG). Gerade vor dem Hintergrund der rasanten dynamischen Fortentwicklung der Informationstechnologie soll durch die Einhaltung dieser Bearbeitungsgrundsätze eine übermässige, zweckwidrige oder unrichtige Datenbearbeitung verhindert werden.

C. Adressat der Pflichten

5 Die sich aus den Bearbeitungsgrundsätzen ergebenden Pflichten treffen in erster Linie den **Verantwortlichen** (Art. 5 lit. j DSG). Der Auftragsbearbeiter bearbeitet Personendaten lediglich im Auftrag des Verantwortlichen (Art. 5 lit. k DSG) und kann sich dabei auf dieselben Rechtfertigungsgründe stützen wie der Verantwortliche (Art. 9 Abs. 4 DSG).

6 Der Auftragsbearbeiter ist als solcher nicht ausdrücklich als Adressat der Bearbeitungsgrundsätze von Art. 6 DSG aufgeführt, anders ist dies der Fall beim (strafbewehrten) Bearbeitungsgrundsatz der Datensicherheit (Art. 8 DSG, Art. 61 lit. c DSG) und bei weiteren Pflichten aus dem DSG, bspw. Art. 12

3. Auch der EDÖB scheint seine bisherige Praxis, nach der er für jede Datenbearbeitung eine rechtliche Grundlage BSK DSG- Bühlmann/Reinle, Art. 6 DSG N. 7 mit Verweis z.B. auf EDÖB, Schlussbericht Microsoft Windows 10 vom 19.8.2016, 18) gemäss seinem neueren Tätigkeitsbericht aufgegeben zu haben (Tätigkeitsbericht 2023/2024 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, Seite 8).
4. Ausnahmen finden sich in Art. 34 Abs. 4 und Art. 36 Abs. 2 DSG.
5. Vgl. Esther Zysset, Kommentierung zu Art. 34 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version: 16.8.2023: https://onlinekommentar.ch/de/kommentare/dsg34 (besucht am 6.5.2024), DOI: 10.17176/20230816-145546-0, N 14 f.
6. Botschaft DSG 1988, S. 449; BSK DSG-Maurer-Lambrou/Steiner, Art. 4 aDSG N. 4 [3. Auflage].
7. BVGer, 10.4.2022, A-4467/2011, E.8.1.1; DSG-Rosenthal/Jöhri, Art. 4 N. 4.
8. Vgl. hierzu die weite Definition des Begriffs „Bearbeiten" in Art. 5 lit. d DSG; Lobsiger, S. 311; vgl. in diesem Zusammenhang auch die Klarstellung des EDÖBs, dass das geltende Datenschutzgesetz auf KI-gestützte Datenbearbeitungen direkt anwendbar ist, abrufbar unter: https://www.edoeb.admin.ch/de/09112023-geltendes-dsg-ist-auf-ki-anwendbar.
9. Botschaft DSG 1988, S. 417.
10. Botschaft DSG 2017, S. 6956.
11. Lobsiger, S. 311 ff.

Abs. 1 DSG, Art. 17 Abs. 2 DSG und beim 3. Kapitel des DSG, welche jeweils explizit den Verantwortlichen und/oder den Auftragsbearbeiter in die Pflicht nehmen.

D. Rechtliche und wirtschaftliche Folgen einer Verletzung

7 Die Bestimmungen der Art. 6 Abs. 3 DSG (Zweckbindung und Transparenz), Art. 6 Abs. 4 DSG (zeitliche Limitierung der Datenbearbeitung) und Art. 6 Abs. 5 DSG (Richtigkeit) sind nicht in dem abschliessenden Katalog der strafbaren Handlungen (Art 60 ff. DSG) aufgeführt. Ein Verstoss gegen diese Bearbeitungsgrundsätze ist für sich genommen selbst dann nicht nach dem DSG strafbar, wenn er nicht gerechtfertigt ist. Trotz umfassender Überarbeitung der strafrechtlichen Bestimmungen wurde im Zuge der Revision des DSG daran nichts geändert.[12] Es droht aber Strafbarkeit bei Verletzung anderer Pflichten, die mit diesen Bearbeitungsgrundsätzen zusammenhängen, zum Beispiel die Informationspflicht, Art. 19, 21 i.V.m. Art. 60 Abs. 1 lit. b DSG. Auch können Straftatbestände ausserhalb des DSG in Betracht kommen.[13]

8 Von ganz erheblicher Bedeutung sind die sich aus dem neuen Datenschutzgesetz ergebenden weiteren **Befugnisse des EDÖB**, welche bei einer Verletzung von Datenschutzvorschriften unter anderem bis hin zu einem **Verbot der Bearbeitungstätigkeiten** oder einer Verfügung zur **Vernichtung der Daten** führen können. Der EDÖB hat in diesem Zusammenhang in seinem Tätigkeitsbericht 2022/2023 bereits angekündigt, seine aufsichtsrechtliche Tätigkeit zu intensivieren und die Anzahl der Untersuchungen zu erhöhen.[14]

9 Zudem kann eine Verletzung Rechtsansprüche nach dem DSG (vor allem nach Art. 32 DSG und Art. 41 DSG) sowie zivilrechtliche Ansprüche wegen Verletzung der Persönlichkeit auslösen (Art. 32 Abs. 2 DSG).

10 Abgesehen von den potenziellen rechtlichen Folgen einer Verletzung der Bearbeitungsgrundsätze sind in der Praxis vor allem der mögliche **Vertrauensverlust** und **Reputationsschaden** zu berücksichtigen, der mit einer Verletzung der Bearbeitungsgrundsätze einher geht und sich langfristig negativ auf die Geschäftsentwicklung auswirken kann.

E. Entstehungsgeschichte der einzelnen Bearbeitungsgrundsätze

1. Grundsatz der Zweckbindung und Transparenz, Art. 6 Abs. 3 DSG

11 Art. 6 Abs. 3 DSG verbindet die Grundsätze der Zweckbindung und der Erkennbarkeit, welche im aDSG in zwei getrennten Absätzen (Art. 4 Abs. 3 aDSG und Art. 4 Abs. 4 aDSG) enthalten waren. Die neue Formulierung soll dem Wortlaut des Art. 5 Abs. 4 lit. b des Übereinkommens 108 plus[15] näherkommen, indem die Personendaten nur für einen «bestimmten» und für die betroffenen Personen «erkennbaren» Zweck verarbeitet werden dürfen. Neu ist auch die Formulierung, dass die Daten nur so bearbeitet werden dürfen, dass es mit diesem Zweck «vereinbar» ist. Die Vorschrift rückt

12. Vgl. zu den Änderungen der strafrechtlichen Bestimmungen Botschaft DSG 2017, S. 7098. Der Bundesrat äusserte im Zusammenhang mit Ausführungen zum Umfang der Verfügungskompetenzen des EDÖB die allgemeine Auffassung, dass die Möglichkeit des Beauftragten, eine von einem Bundesorgan durchgeführte Datenbearbeitung zu untersagen oder auszusetzen, sowie die Stärkung der strafrechtlichen Bestimmungen des DSG wirksam genug seien (Botschaft DSG 2017, S. 6966).
13. Z.B. ein Urkundendelikt (Art. 251 StGB) oder ein strafbarer Verstoss gegen das Gesetz gegen den unlauteren Wettbewerb (vgl. Art. 23 ff. UWG).
14. Tätigkeitsbericht 2022/2023 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, Seite 21.
15. Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, BBl 2020, S. 599 ff., welches am 11.10.2023 in Kraft treten wird.

damit terminologisch dem Art. 5 Abs. 1 lit. b DSGVO näher. Inhaltlich sind damit aber gegenüber dem aDSG keine materiellen Änderungen verbunden. [16]

2. Zeitliche Limitierung der Datenbearbeitung, Art. 6 Abs. 4 DSG

12 Mit Art. 6 Abs. 4 DSG wurde neu ausdrücklich die Pflicht aufgenommen, Personendaten zu vernichten oder zu anonymisieren, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. Dies entspricht den Anforderungen des Übereinkommens 108 plus[17] sowie Art. 4 Abs. 1 lit. e der Richtlinie (EU) 2016/680[18] und Art. 5 Abs. 1 lit. e DSGVO («Speicherbegrenzung»). Diese Pflicht ist ebenfalls nicht neu. Sie ergab sich schon vorher aus dem allgemeinen Verhältnismässigkeitsgrundsatz (Art. 4 Abs. 2 aDSG, Art. 6 Abs. 2 DSG). Mit der expliziten Aufnahme in das Gesetz wollte der Gesetzgeber die besondere Bedeutung der zeitlichen Limitierung der Bearbeitung von Personendaten hervorheben, die sich vor dem Hintergrund der technologischen Entwicklung und der beinahe unbegrenzten Speichermöglichkeiten aufdrängt.[19]

3. Grundsatz der Richtigkeit, Art. 6 Abs. 5 DSG

13 Während der Grundsatz der Richtigkeit der Daten bislang in einem eigenständigen Artikel (Art. 5 aDSG) hervorgehoben war, wurde er neu als Absatz 5 in Artikel 6 DSG integriert, um die wichtigsten Datenschutzgrundsätze in einem Artikel zu vereinen.[20] Vorbild dieses Aufbaus waren Art. 5 des Übereinkommens 108 plus, Art. 4 der Richtlinie (EU) 2016/680 sowie Art. 5 der DSGVO. Das bisher in Art. 5 Abs. 2 aDSG enthaltene Berichtigungsrecht wird neu in Art. 32 DSG geregelt.

II. GEGENSTAND DER BESTIMMUNGEN

A. Grundsatz der Zweckbindung und Transparenz, Art. 6 Abs. 3 DSG

1. Anforderungen

14 Nach dem Grundsatz der Zweckbindung und Transparenz dürfen Personendaten nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden. Sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist, Art. 6 Abs. 3 DSG.

15 Zweckidentität ist nach dem neuen Wortlaut des Gesetzes explizit nicht mehr erforderlich. Die Bearbeitung muss lediglich (fortlaufend) mit dem anfänglichen Zweck *vereinbar* sein. Eine Weiterverarbeitung zu anderen Zwecken ist nur dann zulässig, wenn sie nicht unerwartet ist und nicht als unangebracht oder beanstandbar erachtet werden kann.[21]

16 Den Grundsatz der Zweckbindung hatte das Bundesgericht schon vor dem Inkrafttreten des neuen DSG, mit Urteil vom 18. März 2021,[22] in einem Fall betreffend die Bekanntgabe von Personendaten durch ein Bundesorgan relativiert und festgehalten, dass nicht absolute Zweckidentität gefordert werden kann, da ansonsten die in Art. 19 Abs. 1 aDSG vorgesehene Amtshilfe zu stark eingeschränkt

16. Botschaft DSG 2017, S. 7025.
17. Vgl. Art. 5 Abs. 4 lit. e Übereinkommen 108 plus.
18. Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L 119/89 vom 4.5.2016.
19. Botschaft DSG 2017, S. 7026.
20. Botschaft DSG 2017, S. 7026.
21. Botschaft DSG 2017, S. 7025.
22. BGE 147 II 227.

würde. In jedem Fall müsse der Zweck der Amtshilfe aber zumindest mit dem Zweck der ursprünglichen Beschaffung von Personendaten *vereinbar* sein.[23] Das Bundesgericht hatte damit bereits unter dem aDSG «Vereinbarkeit» der Bearbeitung mit dem ursprünglichen Zweck genügen lassen.

17 Die weitere Voraussetzung der Erkennbarkeit muss sowohl hinsichtlich der Beschaffung der Personendaten als auch hinsichtlich des Zwecks ihrer Bearbeitung gegeben sein.[24] Sie kann schon dann als erfüllt angesehen werden, wenn die Beschaffung der Daten und der Zweck ihrer Bearbeitung aus den Umständen klar ersichtlich ist oder wenn die Bearbeitung gesetzlich vorgesehen ist. Diese Möglichkeit besteht nach wie vor, auch wenn die Begriffe «aus den Umständen ersichtlich» und «oder gesetzlich vorgesehen» aus Art. 4 Abs. 3 aDSG nicht in den Wortlaut des Art. 6 Abs. 3 DSG übernommen wurden.[25]

18 Die Anforderungen an die Erkennbarkeit sind im Einzelfall unter Berücksichtigung der Grundsätze der Verhältnismässigkeit sowie nach Treu und Glauben zu bestimmen, Art. 6 Abs. 2 DSG. Vage, nicht definierte oder unpräzise Bearbeitungszwecke genügen grundsätzlich nicht, wobei diese Eigenschaft wiederum nach dem Umständen beurteilt werden und dabei ein Ausgleich zwischen den Interessen der betroffenen Personen und denen des Verantwortlichen bzw. des Auftragsbearbeiters und der Gesellschaft erfolgen muss.[26] Im Fall «Google Street View» hielt das Bundesgericht bspw. fest, dass dem Grundsatz der Zweckbindung und Transparenz nicht schon dadurch genüge getan würde, wenn die Fahrzeuge von Google, auf welchen Kameras installiert sind, für Passanten und Anwohner sichtbar sind. Der Zweck dieser Fahrzeuge, Strassenzüge (etc.) systematisch abzufahren und abzubilden und die Aufnahmen ohne Zustimmung der Betroffenen im Internet zu veröffentlichen, sei nicht ohne Weiteres erkennbar, auch wenn Google Street View in der Schweizer Bevölkerung einen hohen Bekanntheitsgrad geniesse.[27]

19 Das Erfordernis der Erkennbarkeit hängt eng zusammen mit der Informationspflicht nach Art. 19 ff. DSG. Sie ist damit aber nicht zu verwechseln. Während es sich bei dem Erfordernis der Erkennbarkeit um einen Bearbeitungsgrundsatz handelt, bei dem ein Verstoss allenfalls gerechtfertigt sein kann (Art. 31 DSG), ist dies bei Verletzung der Informationspflicht nicht der Fall.[28] Vielmehr ist eine Verletzung der Informationspflicht gemäss Art. 60 Abs. 1 lit. b DSG strafbar.

2. Beispiele

20 Eine Weiterverarbeitung von Adressen zum **Werbeversand** verstösst gegen den Grundsatz der Zweckbindung und Transparenz, wenn die Adressen ursprünglich in einem ganz anderen Zusammenhang, z.B. im Rahmen einer politischen Kampagne gesammelt wurden. Unzulässig ist auch die Analyse von Personendaten in Bezug auf **Konsumgewohnheiten** (zu anderen Zwecken als der Betrugsbekämpfung) auf Basis von Zahlungen mittels Kredit- oder Kundenkarte ohne Einwilligung der betroffenen Person.[29] Auch die Zustellung von unverlangter E-Mail-Werbung an unbekannte und wahllos zusammengestellte Adressen, welche im Internet gesammelt wurden[30] oder die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch ein Privatunternehmen, stellt eine Verletzung des Grundsatzes der Zweckbindung und Transparenz dar.[31]

---

23. Vgl. BGE 147 II 227 E. 6.4.2.
24. Botschaft DSG 2017, S. 7025.
25. Botschaft DSG 2017, S. 7025.
26. Botschaft DSG 2017, S. 7025.
27. BGE 138 II 346 E. 9.1 («Google Street View»).
28. Es können aber Ausnahmen und Einschränkungen bzgl. der Informationspflicht bestehen (vgl. Art. 20 und 21 DSG).
29. Botschaft DSG 2017, S. 7025.
30. VPB 69.106 E. 5.6.

21 Datenschutzrechtlich zulässig hingegen ist die Verwendung einer Adresse zu Werbezwecken, wenn die betroffene Person ihre Adresse im Hinblick auf den Erhalt einer **Kundenkarte** oder für eine Bestellung (online oder nicht) im Rahmen einer anfänglich erkennbaren Zweckbestimmung übermittelt hat.[32]

22 Bei der Versendung von Werbe-Newslettern müssen darüber hinaus, die sich aus dem Gesetz gegen den unlauteren Wettbewerb ergebenden Voraussetzungen, namentlich Art. 3 Abs. 1 lit. o UWG («**Spam-Artikel**») erfüllt werden. Ein Verstoss dagegen kann zu strafrechtlichen Sanktionen führen. Beim Versand von Newslettern ins Ausland sind zudem das jeweilige **nationale Recht** und die dortigen Usancen zu beachten, aus denen sich noch strengere Anforderungen ergeben können.[33]

23 Eine Datenbearbeitung «auf **Vorrat**» im Sinne einer Datenbearbeitung ohne Zweck, verstösst sowohl gegen den Grundsatz der Verhältnismässigkeit als auch gegen den Grundsatz der Zweckbindung und Transparenz und ist daher rechtswidrig.[34] Zulässig ist in der Schweiz aber bislang nach wie vor die anlasslose Speicherung und Aufbewahrung von **Randdaten der Telekommunikation**.[35] Zulässig, zumindest für eine gewisse Dauer, ist auch die polizeiliche Aufbewahrung von Aufzeichnungen aus der **Überwachung von öffentlichen Plätzen**, bei denen die Daten für allfällige strafrechtliche Ermittlungen erhoben und bearbeitet werden.[36] Anders wiederum erachtete das Bundesgericht den Sachverhalt in Bezug auf den (übermässigen) Einsatz von **Funkwasserzählern**. Hier fehlte es an einem Zweck der Speicherung gewisser Daten und der Erforderlichkeit ihres Aussendens.[37]

24 Bei der **Weitergabe von Daten an Dritte** ist besonders zu berücksichtigen, ob diese Bekanntgabe noch vom ursprünglichen Zweck umfasst ist. Das gilt gerade auch für den Austausch von Daten innerhalb von **Konzernunternehmen**. Mangels eines umfassenden Konzernprivilegs[38] gelten auch Unternehmen des gleichen Konzerns als Dritte, sofern sie die Daten nicht lediglich als Auftragsbearbeiter bearbeiten. Die Abgrenzung zwischen Auftragsbearbeiter und (gemeinsamen) Verantwortlichem ist in der Praxis häufig schwierig. Im Ergebnis ist es entscheidend, das Set-Up konsequent aufzusetzen und transparent zu machen. So ist bspw. im **Bereich HR** zu empfehlen, den Konzernzusammenhang schon im Arbeitsvertrag deutlich zu machen. Bei der Weitergabe von Daten an Dritte ist zudem zu berücksichtigen, dass (nicht nur aber eben gerade auch) der Grundsatz der Zweckbindung auch bei der weiteren Datenbearbeitung durch den Empfänger eingehalten werden muss.

25 Vor besonderen Herausforderungen in Bezug auf die Zweckbindung und Transparenz stehen **Big Data-Anwendungen**[39] wie **Data Warehousing**[40] und **Data Mining**[41], weil es im Wesen von Big

31. BGE 136 II 508 E. 4 und 6.3 («Logistep»).
32. Botschaft 2017, S. 7025.
33. In Deutschland bspw. das so genannte Double-Opt-In- Verfahren, wobei die Nachweis-Anforderungen des BGH zum UWG (BGH I ZR 164/09 Urteil vom 10.2.2011) bei der Protokollierung zu berücksichtigen sind, vgl. auch aktualisierte Fassung der Orientierungshilfe der Datenschutzkonferenz (DSK) vom Februar 2022 zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO).
34. BGE 125 II 473, 476.
35. BGE 144 I 126 E. 5, siehe hierzu aber die aktuelle Beschwerde der Digitalen Gesellschaft vor dem Europäischen Gerichtshof für Menschrechte (EGMR), deren Fortgang verfolgt werden sollte, vgl. hierzu die Webseite der Digitalen Gesellschaft: Vorratsdatenspeicherung in der Schweiz steht vor der Beurteilung durch den Europäischen Gerichtshof für Menschenrechte - Digitale Gesellschaft (digitale-gesellschaft.ch).
36. BGE 133 I 77.
37. BGE 147 I 346, 354 E. 5.5.3.
38. Vgl. aber das neue eingeführte «kleine Konzernprivileg» in Art. 20 Abs. 4 DSG.
39. Unter Big Data ist die Auswertung großer, aus einer Vielzahl unterschiedlicher Quellen stammender unstrukturierter Daten zum Zwecke der Erkennung von Gesetzmäßigkeiten, Korrelationen und Kausalitäten und der Generierung von neuen Informationen und Kontextwissen zu verstehen (Gola/Heckmann DS-GVO/BDSG-Schulz, Art. 6 Rn. 151).

Data-Analysen liegt, dass ihr konkreter Zweck sich erst bei Zusammenführung der Daten aufgrund der neu gewonnenen Erkenntnisse ergibt.[42]

26 Big Data ist auch die wichtigste Grundlage für **künstliche Intelligenz (KI)**, welche damit ebenfalls in ein Spannungsverhältnis mit dem Grundsatz der Zweckbindung und Transparenz rückt. Die Zulässigkeit entsprechender Anwendungen ist im Einzelfall zu prüfen.[43] Oft kann bei der Entwicklung von KI-Systemen und der Eingabe von Trainingsdaten der spätere Verarbeitungszweck noch nicht definiert werden, z.B. wenn der Algorithmus eine Vielzahl von Aufgaben übernehmen kann. Zudem werden üblicherweise Trainingsdaten verwendet, welche ursprünglich zu ganz anderen Zwecken erhoben wurden (bspw. wenn als Trainingsdaten im Internet frei verfügbare Daten verwendet werden). Es kann daher oft zweifelhaft sein, ob deren Verarbeitung noch «vereinbar» mit dem ursprünglichen Zweck ist. Besondere Bedeutung wird hier einer differenzierten Betrachtung der unterschiedlichen Datenbearbeitungen im **AI Lifecycle** (Entwicklung, Eingabe von **Trainingsdaten**, Verwendung des Ergebnisses des KI-Systems «**Output**» etc.) sowie den Rechtfertigungsgründen der Einwilligung, Vertragserfüllung und dem berechtigten Interesse zukommen.[44] Laut Mitteilung des EDÖB müssen Hersteller, Anbieter und Verwender von KI-Systemen zudem die Zwecke, die Funktionsweise und die Datenquellen der auf KI beruhenden Bearbeitungen transparent machen.[45] Konkrete Beispiele für Zweckbestimmungen nach der DSGVO durch Entwickler von KI-Systemen liefert hierzu die französische Aufsichtsbehörde CNIL[46]:

Examples of purposes considered to be explicit and specified:

- Development of a large language model (LLM) able to answer questions, generate text according to context (emails, letters, reports, including computer code), perform translations, summaries and corrections of text, perform text classification, analysis of feelings, etc.;
- Development of a voice recognition model capable of identifying a speaker, his or her language, age, gender, etc.;
- Development of a computer vision model capable of detecting different objects such as vehicles (cars, trucks, scooters, etc.), pedestrians, street furniture (dumpsters, public benches, bicycle shelters, etc.), road signs, tricolor lights, road signs, etc.
- Conversely, the purpose would not be considered as specified enough if it only referred to the type of AI system, without mentioning the technically feasible functionalities and capabilities.

---

40. Beim Data Warehousing werden über einen längeren Zeitraum Daten aus unterschiedlichen Quellen gesammelt, nutzungsbezogen aufbereitet und zeit- sowie funktionsgerecht zur Verfügung gestellt, vgl. Fischer/Bornhauser, S. 433 Fn. 63.
41. Beim Data Mining werden Daten miteinander kombiniert, mit dem Ziel noch nicht vorhandene Informationen zu gewinnen, vgl. Hartmann, S. 158.
42. Specht/Mantz-DSGVO/BDSG-Specht, § 9 Rn. 91.
43. Vgl.
hierzu Mitteilung des EDÖB vom 9.11.2023 «Geltendes Datenschutzgesetz ist auf KI direkt anwendbar», abrufbar unter: https://www.edoeb.admin.ch/de/09112023-geltendes-dsg-ist-auf-ki-anwendbar sowie im Hinblick auf die DSGVO der EU die Checkliste des Bayerischen Landesamts für Datenschutzaufsicht, das Positionspapier der DSK zu empfohlenen technischen und organisatorischen Massnahmen bei der Entwicklung und dem Betrieb von KI-Systemen und den Self-assessment Guide for artificial intelligence (AI) systems der französischen Datenschutzaufsichtsbehörde CNIL, allesamt abrufbar unter: https://www.lda.bayern.de/de/ki.html.
44. Vgl. hierzu auch das Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg.
45. Mitteilung des EDÖB vom 9.11.2023 «Geltendes Datenschutzgesetz ist auf KI direkt anwendbar» abrufbar unter: https://www.edoeb.admin.ch/de/09112023-geltendes-dsg-ist-auf-ki-anwendbar.
46. CNIL, «Defining a purpose» vom 7.6.2024, abrufbar unter: https://www.cnil.fr/en/defining-purpose.

Examples of purposes that are not considered explicit and specified:

- Development of a generative AI model (possible capabilities are not defined);
- Development and improvement of an AI system (neither the type of model nor the possible capabilities are defined);
- Development of a model to identify a person's age (the type is not defined).

Die CNIL empfiehlt aus Gründen der Transparenz in diesem Fall darüber hinaus, dass der Verantwortliche in die Lage sein soll, im Vorfeld die vorhersehbaren Fähigkeiten des KI-Systems zu ermitteln, die die grössten Risiken bergen, der Zweck sich auf die Funktionalitäten bezieht, die von vornherein ausgeschlossen sind und der Zweck so weit wie möglich die Bedingungen für die Nutzung des KI-Systems festlegt.

Gerade auch hinsichtlich Transparenzanforderungen ist zudem der gegebenenfalls auch für Schweizer Unternehmen anwendbare AI Act[47] der EU zu berücksichtigen.

27 Das Potential der Wiederverwendung von Daten für **sekundäre Nutzungszwecke** wurde auch vom Schweizer Gesetzgeber erkannt. Der Nationalrat hat als Zweitrat am 12. Juni 2023 eine Motion zur Schaffung eines **Rahmengesetzes für die Sekundärnutzung** von Daten angenommen. Damit wird der Bundesrat zur Ausarbeitung eines Gesetzes beauftragt, welches das Spannungsfeld zwischen Datenschutz und Datennutzung auflösen und vertrauenswürdige Datenräume schaffen soll.[48]

28 Auf europäischer Ebene sind zudem insbesondere der Data Governance Act[49], der Data Act[50], die Regulierung zum European Health Data Space[51] und, wie bereits erwähnt, der AI Act zu berücksichtigen. Diese können auch für Schweizer Unternehmen Anwendung finden.[52]

3. Empfehlungen zur Umsetzung

29 Die Zwecke der Datenbearbeitung müssen festgelegt, dauerhaft eingehalten und transparent gemacht werden. Letzteres lässt sich in der Praxis in der Regel im Rahmen der ohnehin erforderlichen Datenschutzerklärung, je nach Fallgestaltung zumindest teilweise über Allgemeine Geschäftsbedingungen oder im Wege individueller Kommunikation/Hinweise erreichen. Dabei ist darauf zu achten, dass vage, nicht definierte oder unpräzise Bearbeitungszwecke nicht ausreichend sind.[53] Der Grad der erforderlichen Präzisierung ist im Einzelfall unter Berücksichtigung der

47. VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).
48. Motion 22.3890, aufrufbar unter: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20223890, vgl. zur Veröffentlichung von Daten der öffentlichen Verwaltung auch Art. 10 (Open Government Data) des Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG) sowie das entsprechende Portal der Schweizer Behörden für offene Verwaltungsdaten „opendata.swiss" (abrufbar unter https://opendata.swiss/de).
49. VERORDNUNG (EU) 2022/868 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 30.5.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R0868.
50. VERORDNUNG (EU) 2023/2854 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13.12.2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), abrufbar unter: https://eur-lex.europa.eu/eli/reg/2023/2854/oj?locale=de.
51. Zum Zeitpunkt der Verfassung dieser Kommentierung erst im Entwurfsstadium: Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über den europäischen Raum für Gesundheitsdaten vom 3.5.2022, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197.
52. Vgl. bspw. für den Data Act den Magazinbeitrag Gaul, Der Data Act der EU – und die Schweiz, abrufbar unter: https://www.mme.ch/de-ch/magazin/artikel/der-data-act-der-eu-und-die-schweiz.

Grundsätze der Verhältnismässigkeit sowie nach Treu und Glauben zu bestimmen.[54] Bei der Weitergabe an Dritte empfiehlt sich häufig eine vertragliche Regelung, die Daten nur zu bestimmten Zwecken und rechtmässig zu bearbeiten, einschliesslich einer Verpflichtung zur Schadloshaltung. Zumindest sollte aber ein Hinweis auf die Zweckbindung erfolgen.

B. Zeitliche Limitierung der Datenbearbeitung, Art. 6 Abs. 4 DSG

1. Anforderungen

30 Nach dem Grundsatz der zeitlichen Limitierung der Datenbearbeitung müssen Personendaten **vernichtet** oder **anonymisiert** werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.

31 Gleichwohl kann eine weitere Datenbearbeitung gerechtfertigt sein, Art. 31 Abs. 1 DSG. Das ist insbesondere dann der Fall, wenn **Aufbewahrungspflichten**, beispielsweise die zehnjährige Aufbewahrungspflicht für Geschäftsbücher, Buchungsbelege, den Geschäfts- und Revisionsbericht[55] oder steuerrechtliche Aufbewahrungspflichten[56] erfüllt werden müssen.[57] Ein berechtigtes Interesse an der Aufbewahrung kann sich auch aus potenziellen zukünftigen Rechtsstreitigkeiten und aus Verjährungsvorschriften ergeben.

32 **Vernichten** bedeutet im eigentlichen Sinne die unwiederbringliche Zerstörung bzw. Entfernung der Daten.[58] Bei Daten auf Papier ist dieses zu schreddern oder zu verbrennen und es ist sicherzustellen, dass Dritte keinen Zugang zu den «Relikten» erhalten. Bei elektronischen Daten ist nicht nur relevant, wie diese gespeichert werden, sondern auch, wie diese erhalten wurden. Wurden sie mittels USB-Stick übermittelt, muss der USB-Stick unbrauchbar gemacht werden und zudem sind alle Kopien so zu behandeln, dass die Daten nicht mehr lesbar gemacht werden können. Wurden sie per E-Mail übermittelt, müssen auch allfällige Zwischenspeicherungen dieser E-Mail vernichtet werden. Im Übrigen werden hohe Anforderungen an die Vernichtung gestellt. Übliche Löschbefehle oder eine reine Umformatierung stellen gemäss Botschaft zum DSG kein Vernichten im datenschutzrechtlichen Sinn dar.[59]

33 **Vernichten** erfordert danach mehr als **Löschen**.[60] Gleichwohl wird in der Literatur die Auffassung vertreten, dass es sich bei Art. 6 Abs. 4 DSG um ein redaktionelles Versehen handelt und dem Grundsatz der zeitlichen Limitierung auch durch ein Löschen Genüge getan werden könne.[61] Begründet wird dies mit einer unbedachten Übernahme des Begriffs des Vernichtens aus der bisherigen Regelung in Art. 5 aDSG. Zudem würden die Begriffe des Vernichtens und des Löschens im DSG synonym verwendet.[62] Dem ist nach hiesiger Auffassung sicher dann zuzustimmen, wenn der Begriff des Löschens, der im Übrigen weder im DSG noch in der DSGVO definiert ist, so verstanden wird, dass kein Personenbezug mehr hergestellt werden kann, denn dann ist das DSG mangels Vorliegen von Personendaten per definitionem ohnehin nicht (mehr) anwendbar, Art. 5 lit. a. DSG.

53. Botschaft DSG 2017, S. 7025.
54. Botschaft DSG 2003, S. 2106.
55. Art. 958f des Bundesgesetzes betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches vom 30.3.1911 (SR 220).
56. Vgl. bspw. die 20-jährige Aufbewahrungspflicht gem. Art. 70 Abs. 3 des Bundesgesetzes über die Mehrwertsteuer vom 12.6.2009 (SR 641.20).
57. Botschaft DSG 2017, S. 7073.
58. BVGE 2015/13, Erw. 3.3.4.
59. Botschaft DSG 2017, S. 7021 mit Verweis auf BVGE 2015/13, E. 3.3.4.
60. Botschaft DSG 2017, S. 7021.
61. Rosenthal, digma 2019, S. 190 f.
62. Rosenthal, digma 2019, S. 191.

Nach dem risikobasierten Ansatz des DSG ist dies schon dann der Fall, wenn die Herstellung des Personenbezugs nur mit einem hohen Aufwand möglich wäre, den kein Interessent auf sich nehmen würde.[63] Ob dies beispielsweise auch im Rahmen einer **Archivierung** bejaht werden kann, ist im Einzelfall zu prüfen. Auch organisatorische Massnahmen, wie Zugriffssperren und das Vier-Augen-Prinzip können allenfalls als ausreichende Massnahmen erachtet werden.[64]

34 Dem Grundsatz der zeitlichen Limitierung kann auch durch **Anonymisierung** Genüge getan werden. Unter Anonymisierung ist jede Massnahme zu verstehen, die bewirkt, dass die Identität der betroffenen Personen nicht mehr oder nur noch mit ausserordentlichem Aufwand festgestellt werden kann.[65] Anonymisierung ist nicht mit **Pseudonymisierung** zu verwechseln. Als Pseudonymisierung gilt ein Austauschen des Namens und weiterer Identifikationsmerkmale durch ein anderes Kennzeichen, z.B. einen Platzhalter, mit dem Ziel die Bestimmung der betroffenen Person auszuschliessen oder zu erschweren.[66] Mit anderen Worten kann beim Pseudonymisieren der Personenbezug mit dem zugehörigen Schlüssel wieder hergestellt werden. Das gilt aber nur für denjenigen, der den Schlüssel innehat. Diese **relative Betrachtungsweise** führt dazu, dass für denjenigen, der den Schlüssel nicht innehat und für den praktisch ausgeschlossen ist, den Schlüssel zu erlangen, ebenfalls keine Personendaten vorliegen.[67] Diese relative Betrachtungsweise hat ganz erhebliche Auswirkungen auf die Praxis, weil sie für denjenigen, der keinen Schlüssel hat, aus dem Anwendungsbereich des Datenschutzrechts führt.

2. Empfehlungen zur Umsetzung

35 Die Pflicht zur Vernichtung oder Anonymisierung von Daten kann die Verantwortlichen in der Praxis vor grosse Herausforderungen stellen. In einem ersten Schritt empfiehlt es sich, eine Übersicht über die üblichen Datenbearbeitungen in den jeweiligen Geschäftsbereichen zu gewinnen. Sodann sollten die jeweiligen Aufbewahrungs- und Löschfristen festgelegt werden. Praktischerweise erfolgt dies in übersichtlichen Listen, welche gleichzeitig als interne Richtlinien ausgestaltet sind («Aufbewahrungsrichtlinie»/«Data Retention Policy»).

36 Hilfreich für die Umsetzung ist es, wenn die zur Datenverarbeitung verwendete Software bereits entsprechende Funktionalitäten zur automatisierten Löschung anbietet, wobei zum einen darauf geachtet werden sollte, dass diese in technischer Hinsicht den datenschutzrechtlichen Anforderungen genügen, zum anderen, dass die Pflicht zur Löschung im Rahmen von Auftragsdatenbearbeitungsverträgen mit dem IT-Provider/Cloud-Anbieter auch vertraglich hinreichend abgedeckt wird.

C. Grundsatz der Richtigkeit, Art. 6 Abs. 5 DSG

1. Richtigkeit der Daten

a. Anforderungen

37 Personendaten sind richtig, wenn sie die Umstände und Tatsachen, bezogen auf die betroffene Person, sachgerecht wiedergeben. Sie müssen im Gesamtzusammenhang richtig sein, wobei der Zweck und

63. Botschaft DSG 2017, S. 7019; BGE 136 II 508 E. 3 («Logistep»).
64. Rosenthal, digma, S. 195 f.
65. Botschaft DSG 1988, S. 473; Botschaft DSG 2017, S. 7019.
66. BSK DSG-Bühler, Art. 21 aDSG N. 21 [3. Auflage].
67. HGer ZH HG190107-O vom 4.5.2021 E. 3.2.3.; Rossnagel, S. 245 mit Verweis auf EuGH Breyer, C-582/14, ECLI:EU:C:2016:779, 19.10.2016 mit Anm. Moos/Rothkegel, MMR, 2016, 842, 845; bestätigt wurde der relative Ansatz auch vom EuG, T-557/20, ECLI:EU:T:2023:219, 26.4.2023; Rosenthal, Jusletter vom 17.6.2019, S. 40.

die Art der Bearbeitung zu berücksichtigen sind.[68] Daraus ergibt sich bereits, dass der Begriff der Richtigkeit im Datenschutzrecht nicht absolut zu verstehen ist, sondern dem konkreten Anwendungsfall eine erhebliche Bedeutung zukommt.[69]

38 Auch richtige Personendaten können im Gesamtzusammenhang und unter Berücksichtigung des Bearbeitungszwecks im datenschutzrechtlichen Sinne unrichtig sein, beispielsweise wenn eine Person in einer Datensammlung über die Kreditwürdigkeit als «Betriebene» gespeichert wird, obschon sie während Jahren ihre Rechnungen fristgerecht und korrekt bezahlt hat und es nur zu einer Betreibung gekommen ist, weil die Rechnung an eine falsche Adresse zugestellt worden ist.[70] Andererseits müssen falsche Aussagen nicht unbedingt unrichtig im Sinne des Datenschutzrechts sein.[71] So können gemäss Urteil des Bundesgerichts einzelne Informationen nicht als falsch erachtet werden, wenn die Gesamtheit der Informationen die tatsächlichen Gegebenheiten richtig wiedergeben.[72] Auch können Informationen im Sinne von «Momentaufnahmen» durchaus richtig gewesen sein, selbst dann, wenn sie nachträglich unrichtig werden, beispielsweise wenn in einem Urteil noch ein zwischenzeitlich geänderter Name aufgeführt wird. Hier kommt es entscheidend darauf an, zu welchem Zweck die Daten noch verwendet werden.[73] In diesem Zusammenhang ist der Grundsatz der Richtigkeit insbesondere bei der Tätigkeit von Archiven, Museen, Bibliotheken und anderen Gedächtnisinstitutionen differenziert zu betrachten. Da es die Aufgabe solcher Institutionen ist, Dokumente aller Art zu sammeln, zu erschliessen, zu erhalten und zu vermitteln, dürfen diese dabei nicht verändert werden, weil dies dem Zweck der Archivierung zuwiderlaufen würde. Archive erlauben mit Hilfe von Dokumenten eine Momentaufnahme der Vergangenheit, deren «Richtigkeit» sich allein darauf bezieht, dass die fraglichen Dokumente originalgetreu wiedergeben werden, unabhängig davon, ob dies aus aktueller Perspektive noch als zutreffend erachtet wird.[74] Ebenso bezieht sich der Richtigkeitsanspruch bei polizeilichen Kontrollen nicht auf die objektiv feststellbaren Angaben zu den betroffenen Personen, sondern um die Authentizität des Protokolls. Ausschlaggebend ist, ob die vorhandenen Daten die subjektive Beobachtung der ermächtigten Person zum Zeitpunkt der Vornahme der Bewertung wiedergeben.[75]

39 Die Richtigkeit von Daten kann sich grundsätzlich nur auf **Tatsachen** beziehen, die auch objektiv festgestellt werden können. **Werturteile** sind subjektiv und lassen sich kaum als richtig oder falsch einordnen.[76] Eine Abgrenzung ist dann schwierig, wenn Werturteile und Tatsachen vermischt werden. Dies hat insbesondere im Zusammenhang mit «Fake News» aktuelle Bedeutung gewonnen. Richtig oder falsch kann aber zum Beispiel die Angabe sein, dass ein Werturteil von einer bestimmten Person geäussert oder in einer Akte dokumentiert wurde. Ebenso richtig oder falsch kann auch die Angabe sein, auf wen sich das Werturteil bezieht. Auch die weitere Verwendung der Tatsache des Werturteils richtet sich nach den allgemeinem Bearbeitungsgrundsätzen.[77]

40 Vor besonderen Herausforderungen steht die Einhaltung des Grundsatzes der Datenrichtigkeit in Bezug auf **KI-Systeme**. Gerade bei KI-Systemen, bei denen die **Trainingsdaten** aus öffentlich

68. BGer 1C_187/2023 vom 31.10.2024 E. 4.2; BGer 2C_726/2018 vom 14.10.2019 E. 3.4.
69. BSK DSG- Bühlmann/Reinle, Art. 6 DSG N. 247.
70. BSK DSG-Maurer-Lambrou/Schönbächler, Art. 5 N. 5 f. aDSG [3. Auflage].
71. BSK GWG-Gaul/Isler/Vasella, Art. 33 N. 20.
72. BGer 1A.6/2001 vom 2.5.2001 E. 2c; so auch DSG-Rosenthal/Jöhri, Art. 5 N. 2; BSK DSG- Bühlmann/Reinle, Art. 6 DSG N. 257; a.A. wohl aber noch BSK DSG-Maurer-Lambrou/Schönbächler, Art. 5 aDSG N. 6 [3. Auflage], wonach eine Berichtigung von falschen Einzeltatsachen immer möglich sein müsse.
73. Vgl. Fn. 72.
74. Botschaft DSG 2017, S. 7026 f.
75. Philip Glass, Datenschutzrecht für künstliche Intelligenz in der öffentlichen Verwaltung: Eine Auslegeordnung am Beispiel des Kantons Zürich, S. 216, abrufbar unter: https://digitalcollection.zhaw.ch/handle/11475/26658.
76. BGer 2C_726/2018 vom 14.10.2019 E. 3.4.

zugänglichen Quellen, insbesondere dem Internet bezogen werden, lässt sich die Richtigkeit der Daten oft nicht wirksam überprüfen. Auch die Ergebnisse der Datenbearbeitungen von KI-Systemen («**Output**») können unrichtig sein. Einerseits kann wohl nicht davon ausgegangen werden, dass eine «statistische Richtigkeit» bei Datenbearbeitungen im Zusammenhang mit KI-Systemen grundsätzlich ausreichend ist.[78] Andererseits dürfen an Datenbearbeitungen in Bezug auf KI-Systeme aber auch keine höheren Anforderungen gestellt werden, als an sonstige Datenbearbeitungen, da das DSG grundsätzlich technologieneutral ausgestaltet ist. Das bedeutet, dass die Frage der Datenrichtigkeit auch bei Datenbearbeitungen im Rahmen von KI-Systemen im Einzelfall und unter Berücksichtigung des Gesamtzusammenhangs beurteilt werden muss. Besonders relevant sind dabei der Zweck der Datenbearbeitung und die Bedeutung des Outputs sowie der Erwartungshorizont der Verwender. Entscheidend wird hier in der Praxis eine entsprechende Aufklärung der Nutzer sein. Das damit verbundene Erfordernis der Überprüfung des Outputs sollte sich auch in «**AI Guidelines**» von Unternehmen wiederspiegeln.

41 Allgemein gilt: Das Bearbeiten unrichtiger Daten ist nicht per se eine Persönlichkeitsverletzung. Nur wenn die inkorrekten Angaben durch deren Bearbeitung zu einer Persönlichkeitsverletzung führen, sind sie zu berichtigen oder zu vernichten.[79] Auch der Grundsatz der Richtigkeit gilt nicht absolut. Eine Verletzung kann bei privaten Datenbearbeitern nach Art. 31 DSG gerechtfertigt sein. Bei Bundesorganen kann der Anspruch auf Löschung ebenfalls eingeschränkt sein (vgl. Art. 41 Abs. 3-5 DSG).

b. Beispiele

42 Im Fall der Bearbeitung von **Verdachtsinformationen** über die Begehung möglicher Straftaten steht Art. 6 Abs. 5 DSG einer Bearbeitung so lange nicht entgegen, als die Aussagekraft der entsprechenden Information bekannt ist und der Verdacht nicht als gesicherte Erkenntnis erscheint.[80] **Archivierte E-Mails**, die nach heutigem Kenntnisstand falsche Informationen enthalten, sind im datenschutzrechtlichen Sinne gleichwohl richtig, soweit sie nicht unter der Annahme bearbeitet werden, dass diese noch aktuell sind.[81] Ebenso ist die Aufbewahrung von **Geschäftskorrespondenz** im Rahmen der Aufbewahrungspflicht zulässig, auch wenn sie falsche Angaben enthält. Wird in einer Adressdatenbank eines Vereins eine Hausnummer falsch erfasst, dient die Adressdatenbank aber nicht dem postalischen Versand, sondern nur der Kontrolle des Mitgliederbestandes, ist die Angabe nicht zu berichtigen.[82] In jedem Fall ist aber auch bei einer solchen Datenbearbeitung die Einhaltung der weiteren allgemeinen Bearbeitungsgrundsätze zu prüfen, insbesondere die Grundsätze der Verhältnismässigkeit und Zweckbindung.

77. BGer 1C_187/2023 vom 31.10.2024 E. 4.2; SHK DSG-Baeriswyl, Art. 6 N. 66.
78. Vgl. zur Richtigkeit von Prognosen und Wahrscheinlichkeitsaussagen BSK DSG- Bühlmann/Reinle, Art. 6 DSG N. 251, vgl. zu der Frage, wann eine statistische Richtigkeit ausreichend sein kann, auch die Ausführungen der englischen Aufsichtsbehörde (ICO), What do we need to know about accuracy and statistical accuracy?, abrufbar unter: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-do-we-need-to-know-about-accuracy-and-statistical-accuracy/#:~:text=Improving%20the%20%27statistical%20accuracy%27%20of,an%20output%20of%20the%20system.
79. SHK DSG-Baeriswyl, Art. 6 N. 64, BSK DSG-Bühlmann/Reinle, Art. 6 DSG N. 275.
80. BSK GWG-Gaul/Isler/Vasella, Art. 33 N. 20.
81. DSG-Rosenthal/Jöhri, Art. 5 N. 2 mit Verweis auf BGer 1A.6/2001 vom 2.5.2001, E. 2a und 2c.
82. SHK DSG-Baeriswyl, Art. 6 N. 64.

2. Vergewisserungspflicht, Berichtigungs- und Löschungspflicht

a. Anforderungen

43 Nach dem Grundsatz der Richtigkeit muss sich jede Person, die Personendaten bearbeitet, über deren Richtigkeit vergewissern, Art. 6 Abs. 5 S.1 DSG. Art. 6 Abs. 5 S. 2 DSG hält zudem neu explizit fest, dass alle angemessenen Massnahmen getroffen werden müssen, um unrichtige Daten zu berichtigen, löschen oder zu vernichten. Diese Pflicht vervollständigt die Vergewisserungspflicht, welche ansonsten keinen Sinn machen würde.[83] Der Umfang der Vergewisserungspflicht hängt vom Einzelfall ab. Zu berücksichtigen sind dabei insbesondere der Zweck und Umfang der Bearbeitung sowie die Art der bearbeiteten Daten, inwieweit eine Datenbekanntgabe erfolgt und wie sensitiv diese ist.[84] In diesem Rahmen hat sich auch die Vergewisserungspflicht des Datenbearbeiters zu bewegen.[85] Je höher das Risiko einer Persönlichkeitsverletzung, desto höhere Anforderungen sind auch an die Vergewisserungspflicht zu stellen.[86] Die Vergewisserungspflicht kann damit auch zu einer **Aktualisierungspflicht** führen. [87] Sie beinhaltet aber nicht eine generelle Pflicht zur regelmässigen Überprüfung ohne Anlass.[88]

44 Die Durchführung von Massnahmen zur Vergewisserung kann auch **delegiert** werden, zum Beispiel an die Datenquelle oder einen Auftragsbearbeiter.[89] Wird die Vergewisserungspflicht verletzt, liegt von Gesetzes wegen ein Verstoss gegen die Bearbeitungsgrundsätze und damit eine Persönlichkeitsverletzung vor, Art. 30 Abs. 2 lit. a DSG. Nach dem Sinn und Zweck des Gesetzes, kann eine derartige Pflichtverletzung aber nur Ansprüche auf Berichtigung und Schadenersatz auslösen, wenn die Daten auch tatsächlich unrichtig sind.[90] Welche Massnahmen zu treffen sind, hängt u.a. von Art, Umfang und Zweck der Datenbearbeitung, der Sensitivität der Daten und dem Risiko für die Persönlichkeitsrechte der betroffenen Person, ab. Dies ist wiederum im Einzelfall zu bestimmen.[91] Zudem können den Massnahmen der Berichtigung, Löschung oder Aktualisierung gesetzliche Pflichten entgegenstehen.[92]

b. Beispiele

45 Basiert die Datenbearbeitung zu Marketingzwecken auf **eigenen Angaben der betroffenen Person**, hat der Verantwortliche sich nicht über die Richtigkeit zu vergewissern.[93] Ebenso besteht keine generelle Pflicht, eine Kundenkartei für Marketingzwecke laufend auf veraltete Adressen zu überprüfen.[94] Teilt ein Versicherungsnehmer dem Versicherer aber eine Adressänderung mit, der auch die Änderung des Zivilstandes zu entnehmen ist, hat der Versicherer den Zivilstand nachzutragen, sofern dieser Auswirkungen auf die Ausrichtung der Versicherungsleistung hat.[95] Andererseits sind

83. SHK DSG-BAERISWYL, Art. 6 N. 73.
84. BVGer A-4232/2015 vom 18.4.2017 i.S. Moneyhouse, E. 7.1.
85. BGer 2C_726/2018 vom 14.10.2019, E. 3.4.
86. BVGer A-4232/2015 vom 18.4.2017 i.S. Moneyhouse, E. 7.1; BSK DSG- Bühlmann/Reinle, Art. 6 DSG N. 254.
87. Botschaft DSG 2017, S. 7026.
88. SHK DSG-Baeriswyl, Art. 6 N. 72, BSK DSG- Bühlmann/Reinle, Art. 6 DSG N. 255.
89. DSG-Rosenthal/Jöhri, Art. 5 N. 6.
90. SHK DSG-Baeriswyl, Art. 6 N. 71; DSG-Rosenthal/Jöhri, Art. 5 N. 4.
91. Vgl. SHK DSG-Baeriswyl, Art. 6 N. 74; BSK DSG- Bühlmann/Reinle, Art. 6 DSG N. 259. Dies gilt auch in Bezug auf die Frage, ob eine Informationspflicht gegenüber Dritten, welchen die Daten übermittelt wurden, besteht (BSK DSG-Bühlmann/Reinle, Art. 6 DSG N. 264, wonach eine allgemeine Informationspflicht gegenüber Dritten abgelehnt wird. vgl. zum Meinungsstreit bzgl. des alten DSG aber auch N. 263). Eine Informationspflicht gegenüber Dritten besteht aber für Bundesorgane, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben, Art. 29 DSV.
92. Botschaft DSG 2017. S. 7026.
93. SHK DSG-Baeriswyl, Art. 6 N. 70.
94. DSG-Rosenthal/Jöhri, Art. 5 N. 11.

einmal gemachte Angaben in einer Versicherungspolice nicht weiter zu überprüfen, soweit sie keinen Einfluss auf die Prämie oder die Versicherungsleistung haben.[96] Bei Wirtschaftsauskunfteien ist bezüglich der Überprüfung der Datenbestände insbesondere der Umfang der Daten, das Vorliegen von Persönlichkeitsprofilen und Einwilligungen und die Anzahl der getätigten Abfragen zu berücksichtigen.[97] Möchte eine Versicherung **künstliche Intelligenz** (**KI**) einsetzen, um ein Profil der Kunden zu erstellen, die eine Versicherung abschliessen, und dieses Profil als Grundlage für ihre Entscheidungen bei der Berechnung des Versicherungsrisikos heranziehen, sollten nicht nur Daten von Bestandskunden aus Datenquellen mit korrekten und aktuellen Informationen als Trainingsdaten verwendet werden, sondern auch ein für die Bevölkerung repräsentativer Pool von Kunden herangezogen werden, um Verzerrungen zu vermeiden.[98]

3. Empfehlungen zur Umsetzung

46 Die Anforderungen an die nach Art. 6 Abs. 5 DSG erforderlichen Massnahmen sollten im Verhältnis zu den Risiken und Folgen der konkreten Nutzung stehen. Beispiele zu treffender Massnahmen, welche gleichzeitig zentrale Aspekte im Rahmen der Technikgestaltung nach den Grundsätzen von **Privacy by Design** und **Privacy by Default** darstellen, können sein:

- Überprüfung der Verlässlichkeit der Datenquelle
- Bestimmung des Grads der Richtigkeit anhand der Gesamtumstände des Einzelfalles
- Allenfalls erneute Überprüfungen der Daten in Abhängigkeit der Gesamtumstände und der verschiedenen Phasen der Datenbearbeitung
- Reduzierung falscher Positivergebnisse / falscher Negativergebnisse, um z.B. Fehler bei automatisierter Entscheidungsfindung und beim Einsatz künstlicher Intelligenz zu reduzieren
- Aktualisierung der Daten, falls es für den Zweck der Bearbeitung erforderlich ist
- Implementierung von «self-service» Lösungen, bei denen die betroffenen Personen ihre Daten selbst überprüfen und falls nötig korrigieren können
- Einführung von Plausibilitätskontrollen und Qualitätschecks
- Implementierung automatischer Eingabeüberprüfungen, bspw. zur Vermeidung falscher Eingaben von Postleitzahlen
- Drop-Down Menüs statt Freitexteingaben

47 Aus Sicht der Verantwortlichen empfiehlt es sich zudem, betroffenen Personen vertraglich die Pflicht aufzuerlegen, ihre Daten korrekt anzugeben und aktuell zu halten und eine diesbezügliche Haftung, soweit es möglich ist, auszuschliessen. Grundsätzlich sollte bei externen Datenquellen auch eine Verpflichtung zur Schadloshaltung in Betracht gezogen werden. Je nach Fallgestaltung kann dies im Rahmen eines Gesamtkonzepts, welches die Zuordnung von Daten und Verantwortlichkeiten sowie weitere diesbezügliche Rechte und Pflichten umfasst, berücksichtigt werden.

---

95. SHK DSG-Baeriswyl, Art. 6 N. 72.
96. SHK DSG-Baeriswyl, Art. 6 N. 72.
97. Vgl. BVGer A-4232/2015 vom 18.4.2017 i.S. Moneyhouse, E. 7.3.2, wonach der Betreiber der Auskunftei unter Berücksichtigung der konkreten Umstände des dortigen Falls zu einer Überprüfung des Datenbestandes betreffend Richtigkeit in einem Verhältnis von 5% zu den auf der Plattform getätigten Abfragen verurteilt wurde, wobei die Wahl der Massnahmen freigestellt wurde und als denkbares Beispiel die Überprüfung jeder zwanzigsten Abfrage aufgeführt wurde.
98. Vgl. Leitlinien 4/2019 des Europäischen Datenschutzausschusses zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, S. 28.

LITERATURVERZEICHNIS

Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Auflage, Basel 2014 (zit. BSK DSG-Bearbeiter:in [3. Auflage]) sowie 4. Auflage, Basel 2024 (zit. BSK DSG-Bearbeiter:in).

Basler Kommentar zum Geldwäschereigesetz, Basel 2021 (zit. BSK GWG-Bearbeiter:in).

Fischer Joel A./Bornhauser Jonas, Elektronische Board Portale: Hosted in Switzerland als neuer rechtlicher Qualitätsstandard, GesKR 2016, S. 425-448.

Gola/Heckmann, Datenschutzgrundverordnung/Bundesdatenschutzgesetz, 3. Auflage 2022 (zit. Gola/Heckmann DS-GVO/BDSG-Bearbeiter:in).

Hartmann Damian, Text and Data Mining and Copyright in Switzerland and the European Union, sic! 2023, S. 157-167.

Lobsiger Adrian, Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation, SJZ 119 (2023), S. 311-319.

Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, 2023 (zit. OFK DSG- Bearbeiter:in).

Rosenthal David, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter vom 17.6.2019.

Rosenthal David, Löschen und doch nicht löschen, digma 2019, S. 190-197.

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Rossnagel Alexander, Pseudonymisierung personenbezogener Daten, ZD 2018, 243 ff.; Stämpflis Handkommentar zum Datenschutzgesetz, 2. Auflage (zit. SHK DSG- Bearbeiter:in).

Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019 (zit. Specht/Mantz DSGVO/BDSG-Bearbeiter:in).

MATERIALIENVERZEICHNIS

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II 413 ff. (zit. Botschaft DSG 1988).

Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8.11.2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19.2.2003 BBl 2002 2101 ff. (zit. Botschaft DSG 2003).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.12.2017, BBl 2017 6941 ff. (zit. Botschaft DSG 2017).