Dietmar Jahnel
Angelika Pallwein-Prettner

Datenschutzrecht

4., überarbeitete und aktualisierte Auflage

facultas

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über
http://dnb.d-nb.de abrufbar.

4., überarbeitete und aktualisierte Auflage
facultas, 1050 Wien, Österreich
www.facultas.at, office@facultas.at

Satz: Wandl Multimedia-Agentur, Großweikersdorf
Druck: Facultas Verlags- und Buchhandels AG
Printed in Austria
ISBN 978-3-7089-2503-5

Vorwort zur 4. Auflage

Seit dem Erscheinen der 3. Auflage Anfang des Jahres 2021 hat va die Judikatur zum Datenschutzrecht so richtig den „Turbo" gezündet: So hat der EuGH seither mehr als 50 Vorabentscheidungsverfahren mit datenschutzrechtlichem Bezug erlassen. Auch vom VwGH als österreichisches Höchstgericht im verwaltungsrechtlichen Rechtsschutzweg liegen nunmehr etliche Erkenntnisse vor. Die Rechtsprechungstätigkeit der Datenschutz-Senate des BVwG schließlich ist kaum noch zu überblicken, umfasst sie doch bereits über 1.000 Erkenntnisse.

Diesen Entwicklungen kommt die mit der 3. Auflage eingeführte Konzeption des Lehrbuchs Datenschutzrecht entgegen, bei der wir neben der systematischen Darstellung des Rechtsgebietes auch einen Überblick über die vorliegende Judikatur zu den einzelnen Fragestellungen bieten – und zwar in Form von Entscheidungstabellen mit den Kernaussagen aller Rechtsschutzinstanzen (DSB, BVwG, VwGH, VfGH, OGH und EuGH). Die Besonderheit liegt darin, dass diese in Form von prägnanten Leitsätzen im Fließtext an den jeweils relevanten Stellen eingefügt werden. Die oben genannten Zahlen machen klar, dass es hierbei nicht um eine vollständige Auflistung der vorhandenen Entscheidungen gehen kann. Vielmehr haben wir nach bestem Wissen die jeweils relevantesten Urteile und Erkenntnisse angeführt und überholte Entscheidungen gestrichen. Vollständige Judikaturrecherchen sind ohnedies mit den gängigen Rechtsdatenbanken jederzeit möglich, erfordern aber einen erheblichen, wenn nicht enormen Lese- und Auswertungsaufwand. In unserem Lehrbuch hingegen erhalten Praktiker in den jeweiligen Kapiteln einen schnellen Hinweis auf die wesentlichen Aussagen der aktuellen bzw noch immer relevanten älteren Judikatur, den Studierenden wird entsprechendes Anschauungsmaterial zu den zuvor beschriebenen Fragestellungen geboten.

Für diese vierte Auflage wurde die Rechtslage bis Oktober 2024 berücksichtigt. Unser aufrichtiger Dank gilt wiederum dem Verlag Facultas, insbesondere Herrn Peter Wittmann, für die tolle Unterstützung und angenehme Zusammenarbeit. Wir freuen uns natürlich über Anregungen und Feedback jeder Art.

Salzburg/Wien, Oktober 2024 *Angelika Pallwein-Prettner*
Dietmar Jahnel

Inhaltsverzeichnis

4 Wesentliche Begriffsbestimmungen in der DSGVO

5 Rechtmäßigkeit der Verarbeitung

6 Übermittlung von Daten in Drittländer

7 Transparenz und Betroffenenrechte

8 Datenverarbeitung im Auftrag

9 Publizität und Datensicherheit

10 Selbstregulierung und Zertifizierung

11 Videoüberwachung/Bildverarbeitung

12 Beschäftigtendatenschutz

13 Medienprivileg/Wissenschaftsprivileg

14 Aufsichtsbehörden und europäische Zusammenarbeit

15 Rechtsbehelfe, Haftung und Sanktionen

Abkürzungsverzeichnis

ABGB	Allgemeines Bürgerliches Gesetzbuch
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AngG	Angestelltengesetz
ArbVG	Arbeitsverfassungsgesetz
ASchG	ArbeitnehmerInnenschutzgesetz
AZG	Arbeitszeitgesetz
BAO	Bundesabgabenordnung
BEinstG	Behinderteneinstellungsgesetz
BMJ	Bundesministerium für Justiz
B-VG	Bundes-Verfassungsgesetz
BVwG	Bundesverwaltungsgericht
DSAG 2018	Datenschutz-Anpassungsgesetz 2018
DSB	Datenschutzbehörde
DSFA-AV	Datenschutz-Folgenabschätzung
DSG	Datenschutzgesetz (Novellierung des DSG 2000 durch das DSAG 2018)
DSG 1978	Datenschutzgesetz 1978
DSG 2000	Datenschutzgesetz 2000
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkommission
DS-RL	Datenschutz-Richtlinie (1995)
EDSA	Europäischer Datenschutzausschuss
EFZG	Entgeltfortzahlungsgesetz
EMRK	Europäische Menschrechtskonvention
ErwGr	Erwägungsgrund
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
GRC	Charta der Grundrechte der Europäischen Union
KYC	Know Your Costumer
LVwG	Landesverwaltungsgericht
MedienG	Mediengesetz
OGH	Oberster Gerichtshof
StGB	Strafgesetzbuch
StGG 1867	Staatsgrundgesetz 1867
StPO	Strafprozessordnung
TKG 2021	Telekommunikationsgesetz 2021
UGB	Unternehmensgesetzbuch
UrhG	Urheberrechtsgesetz
UrlG	Urlaubsgesetz
VfGH	Verfassungsgerichtshof
VwGH	Verwaltungsgerichtshof

1 Gegenstand des Datenschutzrechts und Grundrecht auf Datenschutz

1.1 Einführung

Die Bezeichnung „Datenschutz" ist insofern missverständlich, als sie wörtlich genommen nahelegt, dass es dabei um den technischen Schutz von Daten geht. Tatsächlich ist die IT-Sicherheit aber nur ein Teilbereich dieser Materie. Das Hauptziel des Datenschutzrechts besteht vielmehr im **Schutz der Privatsphäre des Menschen** bei der Verarbeitung personenbezogener Daten, insbesondere durch den Schutz vor missbräuchlicher Datenverarbeitung. Gleichzeitig soll aber auch **der freie Datenverkehr** ermöglicht werden. Diese beiden Schutzziele des Datenschutzrechts, die in einem Spannungsverhältnis zueinander stehen, finden sich bereits im Titel der Datenschutz-Grundverordnung („Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG").

1.2 Die historische Entwicklung des Datenschutzrechts in Österreich

Etwa seit Beginn der Siebzigerjahre wird versucht, diese schwer miteinander zu vereinbarenden Ziele in eigenen Datenschutzgesetzen zu regeln. In Österreich war dies das **Datenschutzgesetz 1978**, welches weltweit eine der ersten Kodifizierungen auf dem Gebiet des Datenschutzes darstellte. Es verankerte bereits den Schutz der Privatsphäre durch ein eigenes Grundrecht auf Datenschutz und führte verschiedene Informations- und Abwehrrechte für die von der Datenverarbeitung Betroffenen ein.

In der Praxis zeigte sich jedoch bald, dass die Bürger diese neuen Rechte kaum in Anspruch nahmen. Dies führte in den Achtzigerjahren zu einer neuen Sichtweise des Datenschutzes – nicht mehr als bloßes Abwehrrecht, sondern auch als Gestaltungsrecht. Das im „Volkszählungsurteil" des dtBVerfG 1983 erstmals festgehaltene **Grundrecht auf informationelle Selbstbestimmung** wurde in den folgenden Jahren zum Leitmotiv der europäischen Datenschutzentwicklung.

Die Wende zu einem modernen Datenschutzrecht fand durch die **europäische Datenschutzrichtlinie** (DS-RL; Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) statt. Für Österreich bedeutete dies die Verpflichtung zu einer tiefgreifenden Umgestaltung der Datenschutzvorschriften durch das **DSG 2000**, welches mit etlichen Novellen bis zur direkten Anwendbarkeit der DSGVO in Geltung stand. Mit der DSG-Nov 2014 trat die Datenschutzbehörde

als Kontrollstelle iSd Art 28 Abs 1 der DS-RL an die Stelle der früheren Datenschutzkommission.

EU-Richtlinien (wie die DS-RL) sind primär an die Mitgliedstaaten adressiert und nur bezüglich ihrer Zielsetzung verbindlich. Die einzelnen Mitgliedstaaten sind aber in der Auswahl der Form und der Mittel zur Erreichung dieser Ziele weitgehend frei. Richtlinien bedürfen somit einer innerstaatlichen Umsetzung (zumeist in Form eines nationalen Gesetzgebungsakts) – der Zeitraum für die Umsetzung wird in der Regel in der Richtlinie selbst festgelegt (siehe auch Art 288 Abs 3 AEUV). Anders als EU-Richtlinien sind EU-Verordnungen unmittelbar und direkt anwendbar. Es bedarf keiner innerstaatlichen Umsetzung der Norm.

Aufgrund der unterschiedlichen nationalen Umsetzungen der Datenschutzrichtlinie in den einzelnen Mitgliedstaaten kam es zu einer **Zersplitterung des Datenschutzrechts innerhalb der EU**. Dieser Umstand beeinträchtigte den gemeinsamen Binnenmarkt, insbesondere den notwendigen grenzüberschreitenden Datenaustausch. Auch die unterschiedlichen Zuständigkeiten der jeweiligen Datenschutzbehörden trugen zu einer enormen Bürokratisierung bei, sodass bald schon der Ruf laut wurde, Großteile des Datenschutzrechts innerhalb der EU zu harmonisieren.

Gelungen ist dies – zumindest Großteils – nach mehreren Anläufen mit der **EU-Datenschutz-Grundverordnung** (DSGVO). Am 4. Mai 2016 wurde die DSGVO offiziell im Amtsblatt der Europäischen Union veröffentlicht. Die Verordnung trat am 24. Mai 2016 in Kraft. Nach einer zweijährigen Übergangsfrist wurde die Verordnung am **25. Mai 2018** in der gesamten Europäischen Union **verbindlich und unmittelbar anwendbar**.

Mit dieser neuen Rechtsgrundlage waren zwar zahlreiche Neuerungen im Detail verbunden, die bisher geltenden Grundsätze des europäischen Datenschutzrechts wurden aber durch die DSGVO keineswegs über Bord geworfen, sondern aktualisiert, modernisiert und weiterentwickelt. Die DSGVO besteht aus 99 Artikeln und 173 Erwägungsgründen. Wegen der vielen Kompromisse bei der Textierung des Gesetzestextes der DSGVO und der vielen unbestimmten Rechtsbegriffe (va bei den inhaltlich neuen Bestimmungen) spielen die Erwägungsgründe (ErwGr) bei der Auslegung eine große Rolle (siehe Kapitel 2.1).

Die DSGVO enthält zahlreiche **Öffnungsklauseln**, die den Mitgliedstaaten neben den unmittelbar anwendbaren Bestimmungen an den entsprechenden Stellen einen gewissen Regelungsspielraum einräumen. Sie wird deshalb auch als sog **„hinkende" Verordnung** bezeichnet. In Österreich wurden diese Öffnungsklauseln im neuen **Datenschutzgesetz (DSG)** ausgeführt. In Bereichen, in denen Öffnungsklauseln bestehen, ist daher sowohl der Text der DSGVO als auch der Text des DSG heranzuziehen, um die in Österreich geltende Rechtslage zu eruieren.

Dabei sollte ursprünglich ein völlig neues DSG geschaffen werden, in dem das Grundrecht auf Datenschutz vereinfacht und auf natürliche Personen eingeschränkt sowie eine einheitliche Kompetenzgrundlage für den Bund in den allgemeinen Angelegenheiten des Schutzes personenbezogener Daten einge-

führt werden hätte sollen. Dazu ist es aber mangels Zustandekommens der notwendigen Verfassungsmehrheit weder im **Datenschutz-Anpassungsgesetz 2018** (BGBl I 120/2017) noch im **Datenschutz-Deregulierungs-Gesetz** 2018 (BGBl I 24/2018) gekommen.

Durch BGBl I 14/2019 wurde immerhin eine neue, **einheitliche Kompetenzgrundlage für den Bund** geschaffen. Danach besteht seit 1. Januar 2020 in Art 10 Abs 1 Z 13 die Bundeskompetenz für „allgemeine Angelegenheiten des Schutzes personenbezogener Daten". Durch die Einschränkung auf allgemeine Angelegenheiten des Schutzes personenbezogener Daten bleibt die Zuständigkeit zur Erlassung von auf einen bestimmten Gegenstand bezogenen datenschutzrechtlichen (Sonder)Regelungen – wie bisher auch – unberührt. Die Regelungen betreffend allgemeine Angelegenheiten des Schutzes personenbezogener Daten werden auf den neuen Kompetenztatbestand in Art 10 Abs 1 Z 13 B-VG gestützt. Hingegen können spezifische datenschutzrechtliche Regelungen sowohl in Angelegenheiten der Bundesgesetzgebung als auch in Angelegenheiten der Landesgesetzgebung weiterhin auf Basis der Kompetenztatbestände der jeweiligen Materie erlassen werden (**materienspezifischer Datenschutz** als Annexmaterie). Beispiele dafür sind die sonderdatenschutzrechtlichen Vorschriften in den §§ 51 ff Sicherheitspolizeigesetz (SPG) oder in den Krankenanstaltengesetzen der Länder.

Neben der unmittelbar anwendbaren DSGVO ist die „**Datenschutz-Richtlinie Polizei und Strafjustiz**" RL (EU) 2016/680 für die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung relevant. Diese Richtlinie wurde va im 3. Hauptstück des DSG in den §§ 36 bis 59 ins österreichische Recht umgesetzt.

Bei der **Arbeit mit dem DSG** ist daher zu beachten, dass **weite Teile dieses Gesetzes**, die keine näheren Durchführungs- oder Ausführungsbestimmungen zur DSGVO enthalten, **nur für Datenverarbeitungen für Polizei und Strafjustiz anwendbar sind**, nicht aber für Datenverarbeitungen durch Private oder sonstige öffentliche Stellen. Dies gilt für die §§ 31 – 34 und 36 – 59.

Der bereichspezifische Datenschutz im Telekommunikationssektor wurde durch eine eigene DatenschutzRL für elektronische Kommunikation („**ePrivacy-RL**") geregelt, die ua Vorschriften betreffend Cookies (siehe Kapitel 5.4.3), die Speicherung von Inhaltsdaten und Verkehrsdaten, Rufnummernanzeige, Standortdaten und unerbetene Nachrichten enthält. Die österreichische Umsetzung dieser RL ist im Telekommunikationsgesetz (TKG 2021) zu finden. In diesem Bereich ist eine Neuregelung durch eine eigene „ePrivacy-Verordnung" (seit Jahren) in Vorbereitung.

1.3 Das Grundrecht auf Datenschutz

1.3.1 Europäische Grundrechte auf Datenschutz

Auf europäischer Ebene sieht die **Grundrechtecharta** der EU (GRC) in Art 7 ein Recht auf „Achtung des Privatlebens" und in Art 8 unter dem Titel „Schutz personenbezogener Daten" ein eigenes Grundrecht auf Datenschutz vor.

> **Artikel 8 – Schutz personenbezogener Daten**
> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Nach der Rsp des EuGH ist der persönliche Anwendungsbereich des Art 8 GRC („jede Person") so zu interpretieren, dass juristische Personen vom Schutzbereich des europäischen Grundrechts auf Datenschutz grundsätzlich nicht umfasst sind, außer es findet sich in der Firma der juristischen Person **der Name einer natürlichen Person** (EuGH 09.11.2010, verb Rs C-92/09, C-93/09 [Volker und Markus Schecke und Eifert]). Inhaltlich hat der EuGH in diesem Urteil im Zusammenhang mit der Veröffentlichung personenbezogener Daten über die Empfänger von Agrarbeihilfen die Grundrechtswidrigkeit eines Rechtsakts des Sekundärrechts festgestellt und diesen für ungültig erklärt. Der EuGH wird in Fällen wie diesen als „**Grundrechtsgericht**" tätig, indem er überprüft, ob eine Rechtsgrundlage im Unionsrecht oder im nationalen Recht für eine Verarbeitung den Anforderungen von Art 7 und 8 GRC entspricht. Dies ist nur dann der Fall, wenn die in der jeweiligen Rechtgrundlage vorgesehene Verarbeitung ein im öffentlichen Interesse liegendes Ziel verfolgt und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck steht.

EuGH 21.03.2024, C-61/22 (Landeshauptstadt Wiesbaden)
Die VO (EU) 2019/1157 zur Erhöhung der **Sicherheit der Personalausweise** von Unionsbürgern und der Aufenthaltsdokumente für Unionsbürger und deren Familienangehörige, die ihr Recht auf Freizügigkeit ausüben, durch welche die Mitgliedstaaten verpflichtet werden, in das Speichermedium von Personalausweisen **zwei Fingerabdrücke** in interoperablen digitalen Formaten aufzunehmen, ist mit Art 7 und 8 GRC vereinbar.

EuGH 05.06.2023, C-204/21 (Kommission gg Polen)
Die Republik Polen hat durch die Erlassung einer nationalen Regelung, die **Richter verpflichtet**, eine Erklärung zu ihrer etwaigen **Mitgliedschaft in einem Verein, einer Stiftung oder einer politischen Partei** sowie zu den dort ausgeübten Funktionen abzugeben, und die eine Veröffentlichung der in diesen Erklärungen enthaltenen Angaben im Internet vorsieht, gegen das Recht auf Schutz personenbezogener Daten nach Art 7 und 8 GRC verstoßen.

Auf nationaler Ebene wurde von der DSB klargestellt, dass sich ein Beschwerdeführer nicht nur gegen Verantwortliche des hoheitlichen Bereichs, sondern auch gegen Rechtsträger des privaten Bereichs auf Art 8 GRC berufen kann. Dem europäischen Grundrecht auf Datenschutz nach Art 8 Abs 1 kommt also ebenso wie § 1 DSG **Horizontalwirkung** zu.

DSB 07.03.2019, DSB-D130.033/0003-DSB/2019

Ausgehend von diesen Überlegungen und aufgrund des Umstands, dass die DSGVO auch Verantwortliche des privaten (also des nicht-hoheitlichen) Bereichs direkt verpflichtet, vertritt die Datenschutzbehörde die Ansicht, dass dem Grundrecht auf Datenschutz nach Art 8 Abs 1 der GRC ebenso wie § 1 DSG **Horizontalwirkung** zukommt.

Mit anderen Worten: Da der DSGVO ein allgemeines Grundrecht auf Datenschutz inhärent ist, welches ausdrücklich in Art 8 Abs 1 GRC verankert ist, kann eine betroffene Person im Ergebnis auch gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, eine Beschwerde nach Art 77 Abs 1 DSGVO einbringen und diese Beschwerde auf eine Verletzung von Art 8 Abs 1 GRC stützen. Eine behauptete Verletzung der Grundsätze nach Art 5 und 6 DSGVO kann daher als behauptete Verletzung von Art 8 GRC geltend gemacht werden.

In engem Zusammenhang mit dem Grundrecht auf Datenschutz gemäß § 1 DSG und Art 8 GRC steht das **Grundrecht auf Achtung des Privat- und Familienlebens nach Art 8 EMRK**. Dies schon deshalb, weil in § 1 Abs 2 DSG für einen zulässigen Eingriff in das Grundrecht auf Datenschutz auf die in Art 8 Abs 2 EMRK angeführten Schutzgüter verwiesen wird (siehe dazu Kapitel 1.3.2.1).

> **Artikel 8 – Recht auf Achtung des Privat- und Familienlebens**
> (1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.
> (2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Kurz zusammengefasst beinhaltet der Schutzbereich von Art 8 EMRK neben der **Wohnung** und dem **Briefverkehr** ganz allgemein das **Privat- und Familienleben**. Es ist ein Jedermannsrecht, das neben natürlichen auch juristischen Personen zukommt. Art 8 EMRK ist insofern weiter gefasst als § 1 DSG und Art 8 GRC, als er das Geschehen in der Wohnung und den Inhalt der Korrespondenz ganz unabhängig davon schützt, ob sie über bestimmte oder bestimmbare Personen Auskunft geben.

1.3.2 Grundrecht auf Datenschutz nach § 1 DSG

Die Verfassungsbestimmung des § 1 DSG regelt das Grundrecht auf Datenschutz. Anders als die Überschrift vermuten lässt, gibt es kein einheitliches Grundrecht auf Datenschutz, das Grundrecht besteht vielmehr aus mehreren, unterschiedlichen Rechten. Im Einzelnen sind dies:

1. das Recht auf **Geheimhaltung** personenbezogener Daten (§ 1 Abs 1 DSG),
2. das Recht auf **Auskunft** (§ 1 Abs 3 Z 1 DSG),
3. das Recht auf **Richtigstellung** unrichtiger Daten (§ 1 Abs 3 Z 2 DSG),
4. das Recht auf **Löschung** unzulässiger Weise verarbeiteter Daten (§ 1 Abs 3 Z 2 DSG).

Schutzbereich des Grundrechts

Das Grundrecht auf Geheimhaltung nach § 1 Abs 1 DSG umfasst sämtliche personenbezogenen Daten, unabhängig von der Art ihrer Verwendung, also selbst das gesprochene Wort (vgl dazu zB VwGH 28.02.2018, Ra 2015/04/0087; DSK 20.07.2007, K121.269/0010-DSK/2007). Der Anwendungsbereich der „Begleit"-Grundrechte nach § 1 Abs 3 DSG (Recht auf Auskunft, Richtigstellung und Löschung) ist hingegen enger, weil es sich hier um Daten handeln muss, die automationsunterstützt verarbeitet werden oder zur Verarbeitung in einer manuell geführten Datei bestimmt sind.

Grundsätzlich sind vom Schutzbereich des Grundrechts nur „personenbezogene Daten" umfasst (siehe dazu Kapitel 4.2). Nach dem Wortlaut des § 1 Abs 1 DSG ist das Vorliegen eines „**schutzwürdigen Geheimhaltungsinteresses**" eine weitere Voraussetzung für den Grundrechtsschutz. Nach § 1 Abs 1 Satz 2 DSG besteht dieses Interesse nicht, wenn die Daten allgemein verfügbar oder nicht auf eine Person rückführbar sind. Diese generellen Ausnahmen vom Grundrecht auf Geheimhaltung bei mangelnder Schutzwürdigkeit und allgemeiner Verfügbarkeit werden allerdings von der DSB und den Gerichten im Hinblick auf die DSGVO einschränkend interpretiert.

VwGH 01.02.2024, Ro 2021/04/0016

Anders als die Verfassungsbestimmung des § 1 Abs 1 zweiter Satz DSG enthalten weder Art 8 GRC noch die DSGVO eine Ausnahme für Daten, die **allgemein verfügbar** bzw öffentlich zugänglich sind. Im Hinblick auf den Anwendungsvorrang des Unionsrechts ist somit in einem Fall, der in den Anwendungsbereich der DSGVO und daher des Unionsrechts fällt, eine Datenverarbeitung auch dann nicht vom Recht auf Schutz personenbezogener Daten ausgenommen, wenn es sich um allgemein verfügbare Daten im Sinn des § 1 Abs 1 zweiter Satz DSG handeln sollte.

DSB 23.04.2019, DSB-D123.626/0006-DSB/2018

Nach gefestigter Rsp der Datenschutzbehörde ist die ganz generelle Annahme des Nichtvorliegens einer **Verletzung schutzwürdiger Geheimhaltungsinteressen** für zulässigerweise veröffentlichte Daten nicht mit den Bestimmungen der DSGVO vereinbar.

Schutz von juristischen Personen

Zentraler Ausgangspunkt des Datenschutzrechts ist das allgemeine Grundrecht auf Geheimhaltung personenbezogener Daten. Dieses datenschutzrechtliche „Basisgrundrecht" schützt den Betroffenen vor Ermittlung und Weitergabe seiner Daten. Es ist ein „Jedermannsrecht", das für jede natürliche und juristische Person gilt, unabhängig von der Staatsbürgerschaft. Weil Träger dieses Grundrechts nicht nur Menschen, sondern auch juristische Personen sind, ist damit (in Österreich) auch ein Schutz von Wirtschaftsdaten verbunden. Das Vorhaben, vor Geltungsbeginn der DSGVO das österreichische Grundrecht an den Anwendungsbereich der DSGVO anzupassen und auf natürliche Personen einzuschränken, wurde nicht verwirklicht.

Seit Geltungsbeginn der DSGVO stellte sich die Frage nach dem Anwendungsbereichs des Grundrechts auf Datenschutz nach § 1 DSG, welches im Vergleich zur Regelung im DSG 2000 keine inhaltliche Änderung erfahren hat und daher weiterhin natürliche und juristische Personen gleichermaßen einbezieht. Der persönliche Anwendungsbereich der DSGVO hingegen umfasst nur natürliche Personen.

Die DSB entwickelte zunächst in verfassungskonformer Interpretation den Lösungsansatz, dass **juristischen Personen jedenfalls die in § 1 DSG normierten Rechte zukommen**, nicht aber jene Rechte, die nur in der DSGVO, nicht aber in § 1 DSG Deckung finden (wie etwa das Recht auf Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit). Die DSB hat in mehreren rechtskräftigen Bescheiden auch die Frage, ob eine juristische Person nach § 24 DSG zur Erhebung einer Beschwerde aktiv legitimiert ist, bei rein nationalen Fällen bejaht.

DSB 25.05.2020, 2020-0.191.240

Eine **juristische Person** (hier: eine GmbH) ist aktiv legitimiert, eine Beschwerde nach § 24 DSG vor der Datenschutzbehörde zu erheben, sofern sie eine Verletzung der durch § 1 DSG gewährleisteten Rechte behauptet.

DSB 19.7.2018, DSB-D123.089/0002-DSB/2018

[Hinweis der Datenschutzbehörde: **Grenzüberschreitender Fall**; daher Beurteilung ausschließlich auf Basis der DSGVO]: Zurückweisung der Beschwerde, da die Beschwerdeführerin eine Beschwerde betreffend Verletzung im Recht auf Löschung einbrachte und die zu löschenden Daten sich explizit auf die Beschwerdeführerin als juristische Person (GmbH) beziehen, und da eine juristische Person keine betroffene Person ist, die eine Datenschutzbeschwerde einbringen kann.

In einem jüngeren Erk des BVwG wurde allerdings die gegenteilige Meinung vertreten und die Aktivlegitimation einer juristischen Person zur Erhebung einer Beschwerde an die DSB verneint.

BVwG 19.09.2023, W298 2261568-1

Keine Aktivlegitimation einer GmbH für Beschwerden nach den §§ 1 und 24 DSG. Eine verfassungskonforme Interpretation von § 24 DSG im Sinne einer Erweiterung entgegen dem Normeninhalt und dem expliziten Wortlaut von § 4 Abs 1 DSG, als dass der einfachgesetzliche Teil des DSG auch eine **juristische**

Person aktiv legitimiere, kommt schon deswegen nicht infrage, weil der Wortlaut der Bestimmung unzweideutig ist.

Der VfGH hat zu dieser Frage ausgesprochen, dass die Grundrechtsbestimmungen in § 1 DSG ohne Zweifel nicht nur natürliche Personen, sondern auch juristische Personen als Grundrechtsträger erfassen. Davon ist aber die Frage zu trennen, ob eine juristische Person wegen Verletzung ihrer Grundrechte auf Geheimhaltung, Auskunft, Richtigstellung oder Löschung gemäß § 1 DSG eine Beschwerde an die DSB erheben kann. Diese Frage musste im Beschwerdefall nicht beantwortet werden, weil im konkreten Fall die Finanzmarktaufsicht auch zur Prüfung des Grundrechts auf Datenschutz zuständig war. Damit ist die Frage der **Aktivlegitimation einer juristischen Person nach den §§ 1 und 24 DSG** nach wie vor höchstgerichtlich ungeklärt.

VfGH 12.03.2024, E 3436/2023
Die Datenschutzbehörde ist auf keinen Fall zur Entscheidung über Beschwerden in Zusammenhang mit Veröffentlichungen (Investorenwarnungen) gemäß § 92 Abs 11 Satz 4 WAG 2018 zuständig, sondern die Finanzmarktaufsicht ist zuständig, im administrativen (Rechtsschutz-)Verfahren nach § 92 Abs 11 Satz WAG 2018 zu prüfen, ob die Investorenwarnung gegen jegliche Vorschriften, sohin auch gegen das Grundrecht auf Datenschutz gemäß § 1 DSG, verstößt.

Einschränkung des Grundrechts auf Datenschutz
Das Grundrecht auf Datenschutz wirkt nicht absolut, sondern kann durch bestimmte, nach § 1 Abs 2 DSG zulässige Eingriffe aus folgenden Gründen beschränkt werden:

- Die Verwendung von personenbezogenen Daten liegt im **lebenswichtigen Interesse des Betroffenen**.
- Die Verwendung erfolgt mit seiner **Zustimmung**.
- Die Beschränkungen sind zur Wahrung **überwiegender berechtigter Interessen** eines anderen zulässig.

Die dritte Variante der Beschränkung unterscheidet zwischen dem öffentlichen und dem privaten Bereich: Im privaten Bereich ist für die Zulässigkeit eines Eingriffs in das Grundrecht (nur) eine Interessenabwägung zwischen Eingreifendem und Betroffenem im Einzelfall vorzunehmen. Der Gesetzgeber kann aber auch eine gesetzliche Grundlage vorsehen. Im **öffentlichen Bereich** hingegen bedarf es zusätzlich zu dieser Interessenabwägung immer einer **gesetzlichen Ermächtigung** für den Grundrechtseingriff. Dabei ist der Gesetzgeber an den materiellen Gesetzesvorbehalt des Art 8 Abs 2 EMRK (zB Maßnahmen für die nationale Sicherheit, die öffentliche Ruhe und Ordnung oder zum Schutz der Gesundheit) gebunden. Besonders schutzwürdige Daten (siehe dazu Kapitel 5.6) dürfen zudem nur zur Wahrung wichtiger öffentlicher Interessen verarbeitet werden. Die Gesetze, die zur Verarbeitung solcher Daten ermächtigen, müssen angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen.

Für alle Arten von Beschränkungen gilt, dass der **Eingriff** in das Grundrecht jeweils **nur** in der **gelindesten, zum Ziel führenden Art vorgenommen**