

DIETMAR JAHNEL
ANGELIKA PALLWEIN-PRETTNER

Datenschutzrecht

Neu: Mit Judikaturtabellen (DSB, BVwG, OGH und EuGH)
für einen schnellen Überblick über die Kernaussagen
aller wichtigen Entscheidungen

3., überarbeitete und aktualisierte Auflage

Dietmar Jahnel/Angelika Pallwein-Prettner

•

Datenschutzrecht

**Dietmar Jahnel
Angelika Pallwein-Prettner**

Datenschutzrecht

3., 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.

Copyright © 2021 Facultas Verlags- und Buchhandels AG
3., überarbeitete und aktualisierte Auflage
facultas, 1050 Wien, Österreich

Alle Rechte, insbesondere das Recht der Vervielfältigung und der
Verbreitung sowie der Übersetzung, sind vorbehalten.

Satz: SOLTÉSZ. Die Medienagentur.

Druck: Facultas Verlags- und Buchhandels AG

Printed in Austria

ISBN 978-3-7089-1978-2

Vorwort zur 3. Auflage

Seit dem Geltungsbeginn der EU-Datenschutz-Grundverordnung mit 25. Mai 2018 sind mehr als zweieinhalb Jahre vergangen. Auch wenn der große „Datenschutz-Hype“ des Jahres 2018 inzwischen abgeklungen ist, ist die Bedeutung des Datenschutzrechts in der Praxis der Unternehmen ebenso wie in der Rechtsberatung enorm gestiegen. Dies machen auch die zahlreichen Bescheide der DSB sowie Urteile bzw Erkenntnisse der Zivil- und Verwaltungsgerichte zu datenschutzrechtlichen Fragen deutlich, die inzwischen ergangen sind. Die Menge an Beiträgen mit Bezug zum Datenschutzrecht in der österreichischen Fachliteratur ist kaum mehr zu überblicken.

Diese Entwicklungen haben wir zum Anlass genommen, das bisherige „Manual Datenschutzrecht“ von Grund auf zu überarbeiten und neu zu konzipieren. Mit der 3. Auflage wurde aus einer Einführung in die Grundzüge des Datenschutzrechts ein Lehrbuch zum Datenschutzrecht, das sich vorrangig an alle an der Materie Interessierten wendet, die über juristische Grundkenntnisse verfügen. Dazu wurde der systematische Aufbau etwas angepasst und der Inhalt um ein Kapitel über „Medienprivileg/Wissenschaftsprivileg“ erweitert.

Darüber hinaus wollen wir in unserem Buch einen Überblick über die bereits vorliegende Judikatur zu den einzelnen Fragestellungen bieten, schneller und vor allem präziser, als dies durch eine Internetrecherche möglich ist. Dazu wurden an den relevanten Stellen Entscheidungstabellen mit den Kernaussagen aller Rechtsschutzinstanzen (DSB, BVwG, OGH und EuGH) in Form von prägnanten Leitsätzen eingefügt. Diese Tabellen sind chronologisch sortiert und so konzipiert, dass bei kommenden Neuauflagen die neuesten Judikate zu Beginn angefügt und überholte Entscheidungen gestrichen werden können. Auf diese Weise erhalten Praktiker in den jeweiligen Kapiteln einen schnellen Hinweis auf die wesentlichen Aussagen der aktuellen bzw der relevanten älteren Judikatur, den Studierenden wird entsprechendes Anschauungsmaterial zu den zuvor beschriebenen Fragestellungen geboten.

Für diese dritte Auflage wurde die Rechtslage bis November 2020 berücksichtigt. Wir möchten uns bei Frau Mag. Nina Niederstrasser für ihre tatkräftige Unterstützung bei der Überarbeitung bedanken. Unser aufrichtiger Dank gilt auch dem Verlag Facultas, insbesondere Herrn Peter Wittmann und Frau Carina Glitzner, für die tolle Unterstützung und angenehme Zusammenarbeit. Wir freuen uns natürlich über Anregungen und Feedback jeder Art.

Salzburg/Wien, Jänner 2021

*Angelika Pallwein-Prettner
Dietmar Jahnel*

Vorwort zur 1. Auflage

Liebe Leserin, lieber Leser,

am 25. Mai 2018 findet die neue EU-Datenschutz-Grundverordnung (DSGVO) Anwendung. Gleichzeitig wird das durch das österreichische Datenschutz-Anpassungsgesetz 2018 umfassend novellierte DSG 2000 – künftig wieder unter dem Titel DSG – in Kraft treten.

Man kann zu Recht behaupten, dass durch die neuen Datenschutzbestimmungen kein Stein auf dem anderen bleibt. So wird – nur als beispielhafte Nennung – das Marktortprinzip den Anwendungsbereich europäischen Datenschutzrechts verändern. Das in Österreich bis dato bestehende Datenverarbeitungsregister wird abgeschafft und zunächst noch quasi zu Archivzwecken zur Verfügung gestellt bleiben. Das behördliche Melde- und Genehmigungssystem wird durch umfassende interne Dokumentations- und Transparenzpflichten ersetzt, welche für die Verantwortlichen einen wesentlichen Mehraufwand bedeuten und dazu führen sollen, einen bewussteren und sorgsameren Umgang mit Daten zu bewirken. Weiters festgeschrieben wird eine Art „Datenschutzauditverpflichtung“, die jedenfalls dann durchzuführen ist, wenn die Datenschutzhypothese von betroffenen Personen bei der Verarbeitung derer personenbezogenen Daten einem hohen Risiko ausgesetzt ist (sog. Datenschutz-Folgenabschätzung). Gleichzeitig erfolgt auch ein Umbau der Rechtsschutzbehörden sowie die Festlegung erheblicher Bußgelder bei Datenschutzverletzungen, die massiv über den Rahmen des ursprünglich geltenden DSG 2000 hinausgehen.

Wir hoffen, dass uns Autoren der Spagat gelungen ist, zum einen den Blick auf das Wesentliche zu lenken, zum anderen aber der Leserin und dem Leser auch die eine oder andere unabdingbare detaillierte Information übersichtlich aufzubereiten.

Wir möchten uns besonders beim Verlag Facultas für die umfassende Unterstützung bei der Erstellung dieses Werkes bedanken. Hier möchten wir vor allem Herrn Peter Wittmann sowie dem zuständigen Lektorat unseren Dank aussprechen.

Weiters dürfen wir Herrn Mag. Stefan Frank-Woda von der Rechtsanwaltskanzlei Binder Grösswang für seine kompetente Unterstützung bei der Werkserstellung danken.

Angelika Pallwein-Prettner, Christian Marzi

Der Verlag und die Autorin haben die traurige Pflicht, Sie vom unerwarteten Ableben von Herrn Mag. Christian Marzi unmittelbar vor Drucklegung des vorliegenden Buches zu informieren. Er hat sich mit großem Elan und Freude diesem Werk zugewandt, das er bis zur Druckfreigabe Anfang Dezember 2017 begleiten konnte.

Es möge allen Lesern dienen und ein Andenken an Christian Marzi sein.

*Angelika Pallwein-Prettner
Der Verlag*

Inhaltsverzeichnis

Vorwort zur 3. Auflage.....	5
Vorwort zur 1. Auflage.....	6
Abkürzungsverzeichnis.....	13

1 Gegenstand des Datenschutzrechts und Grundrecht auf Datenschutz

1.1 Einführung	15
1.2 Die historische Entwicklung des Datenschutzrechts in Österreich	15
1.3 Das Grundrecht auf Datenschutz.....	17
1.3.1 Europäische Grundrechte auf Datenschutz	17
1.3.2 Grundrecht auf Datenschutz nach § 1 DSG	19

2 Systematik der DSGVO

2.1 Aufbau und Interpretation	29
2.2 Allgemeine Grundsätze der Datenverarbeitung	30
2.2.1 Vorbemerkungen.....	30
2.2.2 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz.....	31
2.2.3 Zweckbindung.....	33
2.2.4 Datenminimierung, Speicherbegrenzung	34
2.2.5 Richtigkeit.....	36
2.2.6 Integrität und Vertraulichkeit	36
2.2.7 Rechenschaftspflicht.....	37
2.2.8 Technikgestaltung (Privacy by Design).....	37
2.2.9 Datenschutzfreundliche Voreinstellung (Privacy by Default).....	38
2.3 Öffnungsklauseln.....	39

3 Anwendungsbereiche

3.1 Sachlicher Anwendungsbereich	41
3.1.1 Einführung.....	41
3.1.2 Ganz oder teilweise automatisierte Verarbeitung.....	41
3.1.3 Nichtautomatisierte Verarbeitung	41
3.1.4 Ausschlussgründe	43
3.2 Räumlicher Anwendungsbereich	46
3.2.1 Einführung.....	46
3.2.2 Verarbeitung durch Niederlassungen innerhalb der Union	47
3.2.3 Verarbeitung durch Niederlassungen außerhalb der Union	48

3.2.4	Verarbeitung durch diplomatische oder konsularische Vertretungen	49
 4 Wesentliche Begriffsbestimmungen in der DSGVO		
4.1	Allgemeines	51
4.2	Personenbezogene Daten.....	51
4.2.1	Definition	51
4.2.2	Besondere Kategorien personenbezogener Daten.....	54
4.2.3	Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten.....	56
4.2.4	Pseudonymisierung und Anonymisierung	57
4.2.5	Profiling	59
4.3	Verarbeitung.....	59
4.4	Betroffene Person	61
4.5	Verantwortlicher.....	61
4.5.1	Begriff „Verantwortlicher“	61
4.5.2	Gemeinsam Verantwortliche	62
4.5.3	Entscheidung über Zwecke und Mittel.....	63
4.6	Auftragsverarbeiter	65
 5 Rechtmäßigkeit der Verarbeitung		
5.1	Vorbemerkungen.....	69
5.2	Verbotsprinzip	69
5.3	Erlaubnistatbestände	69
5.4	Die einzelnen Rechtmäßigkeitstatbestände	70
5.4.1	Vorbemerkung	70
5.4.2	Einwilligung (lit a)	71
5.4.3	Exkurs: Cookies	77
5.4.4	Vertragserfüllung (lit b).....	77
5.4.5	Erfüllung einer rechtlichen Verpflichtung (lit c).....	78
5.4.6	Schutz lebenswichtiger Interessen (lit d).....	79
5.4.7	Öffentliches Interesse oder Ausübung öffentlicher Gewalt (lit e)	79
5.4.8	Wahrung berechtigter Interessen (lit f).....	81
5.5	Nationales Datenschutzrecht („Flexibilisierungsklausel“).....	83
5.6	Strafrechtlich relevante Daten	84
5.7	Besondere Kategorien personenbezogener Daten.....	85
5.8	Weiterverwendung für einen anderen Zweck	87
5.9	Prüfschema für die Zulässigkeit einer Datenanwendung.....	89
 6 Übermittlung von Daten in Drittländer		
6.1	Allgemeine Grundsätze der Datenübermittlung in Drittländer	91
6.2	Angemessenheitsbeschluss	92

6.2.1	Gleichgestellte Drittländer	92
6.2.2	Safe Harbor/EU-US Privacy Shield.....	93
6.3	Datenübermittlung vorbehaltlich geeigneter Garantien	94
6.4	Verbindliche unternehmensinterne Datenschutzregelungen	96
6.5	Ausnahmen gemäß Art 49 DSGVO	97
6.6	Ausnahmeklausel.....	99
6.7	Genehmigungsverfahren	100

7 Transparenz und Betroffenenrechte

7.1	Allgemeines	101
7.2	Form und Fristen	101
7.3	Informationspflicht	102
7.3.1	Zweck und Inhalt.....	102
7.3.2	Direkterhebung von Daten	102
7.3.3	Datenerhebung nicht bei der betroffenen Person.....	105
7.3.4	Information durch standardisierte Bildsymbole.....	106
7.4	Recht auf Auskunft.....	107
7.4.1	Form des Auskunftsbegehrens, Identitätsnachweis	107
7.4.2	Inhalt und Form der Auskunftserteilung	108
7.4.3	Frist.....	109
7.4.4	Mitwirkungspflicht	110
7.4.5	Unentgeltlichkeit	110
7.4.6	Beschränkungen des Auskunftsrechts	110
7.5	Berichtigung und Löschung	111
7.5.1	Berichtigungsrecht.....	111
7.5.2	Löschungsrecht („Recht auf Vergessenwerden“)......	111
7.5.3	Folgen der Löschungspflicht	114
7.5.4	Ausnahmen von der Löschungspflicht.....	115
7.5.5	Mitteilungspflicht.....	115
7.6	Exkurs: Rechtssache „Google Spain und Google“	115
7.7	Recht auf Einschränkung der Verarbeitung.....	116
7.8	Recht auf Datenportabilität.....	117
7.9	Widerspruchsrecht.....	118
7.10	Automatisierte Entscheidungen – Profiling	119

8 Datenverarbeitung im Auftrag

8.1	Allgemeines zur Auftragsverarbeitung	123
8.2	Beauftragung eines Auftragsverarbeiters	125
8.3	Beauftragung eines Sub-Auftragsverarbeiters.....	125
8.4	Auftragsverarbeitungsvertrag	126
8.5	Pflichten des Auftragsverarbeiters.....	128
8.6	Befugnisüberschreitung	129
8.7	Haftung.....	129
8.8	Weisungsgebundenheit	130

9 Publizität und Datensicherheit

9.1	Einleitung	131
9.2	Verzeichnis der Verarbeitungstätigkeiten	132
9.2.1	Verarbeitungsverzeichnis des Verantwortlichen	132
9.2.2	Verarbeitungsverzeichnis des Auftragsverarbeiters	133
9.2.3	Aktualisierung des Verarbeitungsverzeichnisses	133
9.3	Datenschutz-Folgenabschätzung	133
9.3.1	Kriterien der Durchführung der Datenschutz-Folgenabschätzung	133
9.3.2	Verfahrensablauf der Datenschutz-Folgenabschätzung	135
9.4	Technische und organisatorische Maßnahmen (TOM)	136
9.5	Meldepflichten bei Datenschutzverletzungen	138
9.6	Datenschutzbeauftragter	141

10 Selbstregulierung und Zertifizierung

10.1	Einleitung	145
10.2	Selbstregulierung durch Verhaltensregeln	146
10.2.1	Allgemeines	146
10.2.2	Inhalt von Verhaltensregeln	147
10.2.3	Genehmigung von Verhaltensregeln	148
10.2.4	Verhaltensregeln in Österreich	148
10.2.5	Sanktionen	149
10.3	Zertifizierungen	149

11 Videoüberwachung/Bildverarbeitung

11.1	Allgemeines	151
11.2	Judikaturdivergenz	152
11.3	Begriff der Bildaufnahme	152
11.4	Zulässigkeit einer Bildaufnahme	153
11.5	Speicherdauer und Kennzeichnung	154

12 Beschäftigtendatenschutz

12.1	Vorbemerkungen	157
12.2	Gesetzliche Grundlagen	157
12.2.1	Europarechtliche Vorgabe	157
12.2.2	Umsetzung in Österreich	158
12.3	Rechtmäßigkeit der Verarbeitung im Beschäftigungskontext	160
12.3.1	Allgemeines	160
12.3.2	Vertragserfüllung und Erfüllung einer rechtlichen Verpflichtung	161
12.3.3	Wahrung berechtigter Interessen	162
12.3.4	Einwilligung	162

12.3.5 Betriebsvereinbarungen	163
12.3.6 Verarbeitung besonderer Kategorien personen- bezogener Daten im Beschäftigungskontext	167
12.4 Datenverarbeitung durch den Betriebsrat.....	169
12.5 Datenminimierung und Speicherung im Beschäftigungskontext ...	172
12.6 Datengeheimnis	173
12.7 Exkurs: Bewerber.....	174

13 Medienprivileg/Wissenschaftsprivileg

13.1 Medienprivileg.....	177
13.1.1 Allgemeines	177
13.1.2 Journalistische Zwecke	178
13.1.3 Wissenschaftliche, künstlerische oder literarische Zwecke	179
13.1.4 § 9 DSGVO.....	179
13.2 Wissenschaftsprivileg.....	181
13.2.1 Allgemeines	181
13.2.2 Öffnungsklausel für wissenschaftliche Forschung.....	182
13.2.3 § 7 DSGVO.....	183
13.2.4 Forschungsorganisationsgesetz (FOG)	183

14 Aufsichtsbehörden und europäische Zusammenarbeit

14.1 Datenschutzbehörde	185
14.1.1 Allgemeines	185
14.1.2 Organisation	185
14.1.3 Aufgaben	187
14.1.4 Befugnisse	188
14.1.5 Ausschluss der Aufsicht über Gerichte.....	191
14.2 Datenschutzrat.....	191
14.2.1 Aufgaben	191
14.2.2 Zusammensetzung	192
14.2.3 Verfahrensweise.....	192
14.3 Europäischer Datenschutzausschuss (EDSA).....	193
14.3.1 Allgemeines	193
14.3.2 Zusammensetzung	193
14.3.3 Verfahrensweise.....	193
14.3.4 Organe	194
14.3.5 Aufgaben des Datenschutzausschusses	194
14.4 Exkurs: Europäischer Datenschutzbeauftragter.....	195
14.5 Zuständigkeit, Zusammenarbeit und Kohärenzverfahren.....	196
14.5.1 Allgemeine Zuständigkeit (Art 55)	196
14.5.2 Zuständigkeit bei grenzüberschreitender Verarbeitung (Art 56)	197

14.5.3	Prüfungsschema Zuständigkeit.....	199
14.5.4	Zusammenarbeit der Aufsichtsbehörden.....	199
14.5.5	Kohärenzverfahren.....	202
14.6	Zusammenarbeit von Verantwortlichem und Auftragsverarbeiter mit Aufsichtsbehörden.....	205

15 Rechtsbehelfe, Haftung und Sanktionen

15.1	Vorbemerkungen.....	207
15.2	Rechtsbehelfe	207
15.2.1	Beschwerde.....	207
15.2.2	Gerichtlicher Rechtsbehelf gegen Aufsichtsbehörden.....	210
15.2.3	Gerichtlicher Rechtsbehelf gegen Verantwortliche	211
15.2.4	Vertretung von betroffenen Personen	213
15.2.5	Aussetzung des Verfahrens.....	213
15.3	Haftung und Recht auf Schadenersatz	214
15.4	Geldbußen.....	217
15.4.1	Vorbemerkungen.....	217
15.4.2	Höhe der Geldbußen	218
15.4.3	Strafbemessung.....	220
15.4.4	Andere Sanktionen.....	222
15.4.5	Haftung für Geldbußen.....	224
	Weiterführende Literatur und sonstige Arbeitsbehelfe	227
	Stichwortverzeichnis	231

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
BMVRDJ	Bundesministerium für Verfassung, Reformen, Deregulierung und 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 Menschenrechtskonvention
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 2003	Telekommunikationsgesetz 2003
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 **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. Durch die DSG-Nov 2010 wurde ein neues Kapitel über Videoüberwachung und ein elektronisches Meldeverfahren eingeführt. Mit der

DSG-Nov 2014 trat die Datenschutzbehörde als Kontrollstelle iSd Art 28 Abs 1 der DS-RL an die Stelle der bisherigen Datenschutzkommission.

EU-Richtlinien 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 eingeführt werden hätte sollen. Dazu ist es aber mangels Zustandekommens der notwendigen Verfassungsmehrheit weder im **Datenschutz-Anpassungsge-**

setz 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.

Mit Inkrafttreten der neuen Kompetenzbestimmung am 1. Jänner 2020 traten sowohl die Verfassungsbestimmungen der §§ 2 und 3 DSG als auch die bislang bestehenden Landesdatenschutzgesetze in allgemeinen Angelegenheiten des Schutzes personenbezogener Daten im nicht-automationsunterstützten Datenverkehr außer Kraft.

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.

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.

Von der DSB wurde 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.

Artikel 1 (Verfassungsbestimmung)

Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne

Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
 2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.
- (4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

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).

Mit Anwendbarkeit der Bestimmungen der DSGVO stellte sich die Frage des Schutzbereichs des Grundrechts auf Datenschutz nach § 1 DSG, welches im Vergleich zur Regelung im DSG 2000 keine inhaltliche Änderung erfahren hatte und daher weiterhin natürliche und juristische Personen gleichermaßen einbezieht. Der persönliche Schutzbereich der DSGVO hingegen umfasst nur natürliche Personen.

Die DSB entwickelte in ihrer Rechtsprechung den Lösungsansatz, eine verfassungskonforme Interpretation führe dazu, 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).



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 13.09.2018, DSB-D216.713/0006-DSB/2018

Zwar schützt die DSGVO selbst nur natürliche Personen, jedoch ist in verfassungskonformer Interpretation davon auszugehen, dass die in § 1 DSG normierten Rechte **auch juristischen Personen** zukommen und diese sich folglich darauf berufen können. Da es sich bei der Beschwerdeführerin um eine juristische Person handelt, kann diese durch die Videoüberwachung denkunmöglich im Recht auf Geheimhaltung nach § 1 DSG verletzt werden, weil keine Daten der Beschwerdeführerin verarbeitet werden.

Dies hat zur Folge, dass sich juristische Personen (allerdings nur bei rein österreichischen Sachverhalten!) wegen einer behaupteten Verletzung in den Rechten auf Geheimhaltung, Auskunft, Richtigstellung und Löschung auf das

Grundrecht auf Datenschutz berufen und dieses vor der Datenschutzbehörde oder vor Gericht geltend machen können.



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.

1.3.2.1 Recht auf Geheimhaltung personenbezogener Daten

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. Wie erwähnt gab es allerdings bereits mehrere – bislang gescheiterte – Versuche, das österreichische Grundrecht an den Anwendungsbereich der DSGVO anzupassen und auf natürliche Personen einzuschränken.

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**“ 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. Damit sollte klargestellt werden, dass kein „Quellenschutz“ besteht und jedermann auf öffentliche Daten zugreifen und von ihnen Kenntnis nehmen darf. Sollten aber durch die Weiterverwendung allgemein zugänglicher Daten „neue“ Informationen entstehen, ist die Zulässigkeit ihrer Generierung nach den rechtlichen Voraussetzungen der Art 5–9 DSGVO neu zu beurteilen. Der explizite Ausschluss der Schutzwürdigkeit von nicht auf eine Person rückführbare Daten stellt auf die Fälle ab, in denen zwar nicht der Verantwortliche selbst, aber Dritte die Betroffenen identifizieren können, also auf „pseudonymisierte Daten“. Diese generellen Ausnahmen vom Grundrecht auf Geheimhaltung werden allerdings von der DSB im Hinblick auf die DSGVO einschränkend interpretiert.



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.

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 Betroffenen 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** werden darf. Nach der Rsp des VfGH muss jeder Grundrechtseingriff also verhältnismäßig sein, wobei das Element der Erforderlichkeit in § 1 Abs 2 letzter Satz besonders hervorgehoben wird. Zusätzlich verlangt der VfGH bei Eingriffsgesetzen eine ausreichende Bestimmtheit.

Bei der Frage, ob ein Eingriff in das Grundrecht auf Datenschutz gerechtfertigt ist oder nicht, ist zu unterscheiden, ob der **Eingriff durch den Gesetzgeber** oder **eine konkrete Datenverarbeitung** erfolgt. Im ersten Fall hat der VfGH die Verfassungskonformität **der gesetzlichen Grundlage für Datenverarbeitungen** zu beurteilen und das Gesetz allenfalls aufzuheben.

In folgenden Fällen hat der VfGH eine Verletzung des Grundrechts auf Geheimhaltung ausgesprochen und **die gesetzlichen Grundlagen aufgehoben**:



VfGH 12.12.2019, G 164/2019

Verletzung im Recht auf Geheimhaltung durch die Verpflichtung "sämtlicher Behörden" zur Übermittlung personenbezogener Daten an die Länder in § 1 Abs 1 und 2 **Sozialhilfe-Statistikgesetz**.

VfGH 11.12.2019, G 72/2019, G 181/2019

Kfz-Kennzeichenerfassung und Bundestrojaner sind ua wegen der Verletzung von Art 8 Abs 2 MRK und § 1 DSG verfassungswidrig. Aufhebung von § 54 Abs 4b und § 57 Abs 2a **SPG** und § 98a Abs 2 erster Satz **StVO**.

VfSlg 19.892/2014

Verfassungswidrigkeit von Bestimmungen des **TKG 2003, der StPO und des SPG** über die **Vorratsdatenspeicherung** wegen unverhältnismäßigen Eingriffs in das Grundrecht auf Datenschutz und das Recht auf Privat- und Familienleben. Die Regelung über die Löschung von Daten ist nicht in einer Weise bestimmt, die dem Erfordernis einer gesetzlichen Regelung iSd § 1 Abs 2 DSG 2000 entspricht.

VfSlg 19.886/2014

Verfassungswidrigkeit von § 65 Abs 1 **SPG** idF BGBl I 13/2012 betreffend die Voraussetzungen für eine erkennungsdienstliche Behandlung, weil der Eingriff in das Grundrecht auf Datenschutz nicht hinreichend konkretisiert und begrenzt war.

VfSlg 19.801/2013

Aufhebung von § 140 Abs 3 **StPO** über die Verwendung von im Strafverfahren ermittelten personenbezogenen Daten als Beweismittel in anderen gerichtlichen und verwaltungsbehördlichen Verfahren wegen Verstoßes gegen das Grundrecht auf Datenschutz. Fehlen einer ausdrücklichen gesetzlichen Ermächtigung für eine Weiterverwendung dieser Daten.

VfSlg 19.738/2013

Die Regelung des § 67 Abs 1 erster Satz **SPG** über die Voraussetzung zur Ermittlung von DNA-Daten ist nicht hinreichend differenziert und nicht ausreichend präzise und daher verfassungswidrig.

VfSlg 12.228/1989

Die umfassende Veröffentlichungspflicht von Wirtschaftsdaten nach § 8 Abs 1 **BundesstatistikG** hat das Grundrecht auf Datenschutz verletzt.

In folgenden Fällen lag nach Ansicht des VfGH keine Verletzung des Grundrechts auf Datenschutz **durch ein Gesetz** vor:



VfSlg 19673/2012

Keine Verletzung im Recht auf Datenschutz durch Anordnung der **Übermittlung bestimmter Wirtschaftsdaten** von Elektrizitätsunternehmen **an die E-Control** zum Zweck einer Marktuntersuchung. Die gesetzliche Ermächtigung zur Datenerhebung im Zusammenhang mit den der E-Control als Regulierungsbehörde übertragenen Aufgaben der Überwachung und Aufsicht über den Elektrizitätsmarkt ist hinreichend determiniert.

VfSlg 19659/2012

Keine Verfassungswidrigkeit der in § 75 Abs 3 **StPO** angeordneten **Speicherfrist** von 60 Jahren für strafrechtsrelevante Daten.

VfSlg 18146/2007

Kein Verstoß der Regelung in der **StVO** über das automatische Geschwindigkeitsmesssystem **Section Control** gegen das Grundrecht auf Datenschutz.
