



Republik Österreich

Datenschutz
behörde

Datenschutzbericht 2019



Datenschutzbericht 2019

Wien, im März 2020

Impressum

Medieninhaber, Herausgeber und Redaktion:

Datenschutzbehörde, Dr. Andrea Jelinek

(gemäß § 18ff DSGVO), Barichgasse 40-42, 1030 Wien

Kontakt: dsb@dsb.gv.at

Website: www.dsb.gv.at

Fotonachweis: Stefanie Korherr (Seite 6)

Gestaltung: Datenschutzbehörde

Druck: BMVRDJ

Wien, 2020

Inhalt

1 Vorwort	6
2 Die Datenschutzbehörde	7
2.1 Organisation und Aufgaben.....	7
2.1.1 Die Datenschutzbehörde.....	7
2.1.2 Aufgaben und Befugnisse.....	7
2.2 Der Personalstand.....	8
3 Tätigkeit der Datenschutzbehörde	8
3.1 Statistische Darstellung.....	8
3.2 Verfahren und Auskünfte.....	13
3.2.1.1 Individualbeschwerden Inland.....	13
3.2.1.2 Grenzüberschreitende Fälle der DSB.....	37
3.2.2 Rechtsauskünfte an Bürgerinnen und Bürger.....	38
3.2.3 Genehmigungen im Internationalen Datenverkehr.....	38
3.2.4 Genehmigungen nach §§ 7 u. 8 DSG.....	39
3.2.5 Amtswegige Prüfverfahren.....	40
3.2.6 Beschwerdeverfahren vor dem Bundesverwaltungsgericht einschließlich Säumnis- beschwerden.....	41
3.2.6a Beschwerdeverfahren vor dem Bundesverwaltungsgericht in Verwaltungsstrafsa- chen.....	44
3.2.7 Verfahren über die Meldung der Verletzung des Schutzes personenbezogener Daten	47
3.2.8 Konsultationsverfahren.....	48
3.2.9 Anträge auf Genehmigung von Verhaltensregeln.....	49
3.2.10 Die Verhängung von Geldbußen durch die Österreichische Datenschutzbehörde.....	50
3.2.11 Stellungnahmen zu Gesetzes- und Verordnungsentwürfen.....	51
4 Wesentliche höchstgerichtliche Entscheidungen	52

4.1 Verfahren vor dem Verfassungsgerichtshof.....	52
4.2 Oberster Gerichtshof.....	54
4.2.1 Videoaufnahmen einer Amtshandlung zu Zwecken der Beweisaufnahme zulässig, nicht aber deren Veröffentlichung (§§ 16 ABGB, 78 UrhG)	54
4.2.2 Oberster Gerichtshof in 6 Nc30/19t, Privat gg. Republik Österreich wegen Veröffent- lichung eines OGH Disziplinarerkenntnisses im RIS.....	55
4.2.3 Parallele Zuständigkeit der Gerichte und Aufsichtsbehörden nach der DSGVO möglich (6 Ob 91/19d).....	56
4.2.4 Videoaufnahmen im Lichte der §§ 12, 13 DSG (6 Ob 150/19f).....	57
4.3 Verwaltungsgerichtshof.....	58
4.3.1 VwGH, Ra 2017/04/0141, 17. Dezember 2019.....	58
4.3.2 VwGH, Ra 2017/04/0145; 30.04.2019.....	59
4.3.3 VwGH, Ra 2017/04/0134, 30. April 2019.....	60
4.3.4 VwGH, Ra 2018/04/0194, 22. März 2019.....	60
4.4 Europäischer Gerichtshof für Menschenrechte.....	61
4.4.1 EGMR, Catt v. the United Kingdom, 24.01.2019 – 43514/15.....	61
4.4.2 EGMR, López Ribalda and Others v. Spain, 17.10.2019 – 1874/13 und 8567/13.....	61
4.4.3 EGMR, Hambardzumyan v. Armenia, 05.12.2019 – 43478/11.....	62
4.5 Europäischer Gerichtshof.....	62
4.5.1 Urteil vom 14. Februar 2019, C-345/17 (Buivids).....	62
4.5.2 Urteil vom 29. Juli 2019, C-40/17 (Fashion ID).....	63
4.5.3 Urteil vom 24. September 2019, C-507/17 (Google LLC gg. CNIL).....	63
4.5.4 Urteil vom 24. September 2019, C-136/17 (GC u.a gg. CNIL).....	64
4.5.5 Urteil vom 1. Oktober 2019, C-673/17 (Planet 49).....	65
4.5.6 Urteil vom 11. Dezember 2019, C-708/18 (TK).....	65
5 Datenschutz-Grundverordnung und Datenschutzgesetz – Erfahrungen und legitime Maßnah- men.....	66
5.1 Erfahrungen der DSB im Berichtszeitraum.....	66

5.1.1 Verfahrenszahlen und Personalstand.....	66
5.1.2 Gliederung der DSB.....	67
5.1.3 Verwaltungsstrafverfahren.....	67
5.1.4. Grenzüberschreitende Zusammenarbeit.....	68
5.2 Verordnung über Überwachungsstellen zur Einhaltung von Verhaltensregeln gemäß Art. 41 DSGVO.....	68
5.3 Novelle des DSG im Jahr 2019 und weiterer Anpassungsbedarf.....	68
6 Europäische Zusammenarbeit.....	70
6.1 Europäische Union.....	70
6.1.1 Der Europäische Datenschutzausschuss.....	70
6.1.2 Europol.....	71
6.1.3 Schengen.....	71
6.1.4 Zoll.....	72
6.1.5 Eurodac.....	72
6.1.6 Visa.....	72
6.2 Europarat.....	73
7 Internationale Beziehungen.....	73
EU-U.S. Privacy Shield – 3rd Annual Joint Review.....	73
Nachruf auf Hofrat Mag. Georg Lechner und Mag. Samraa El Fohail.....	74

1 Vorwort



Die unabhängige Datenschutzbehörde (DSB) ist seit 1. Jänner 2014 die nationale Kontrollstelle im Sinne des Art. 28 der Datenschutzrichtlinie 95/46/EG und nimmt seit 25. Mai 2018 diese Aufgabe aufgrund § 18 Datenschutzgesetz (iVm Art. 51 DSGVO) wahr. Der Datenschutzbehörde obliegt die Führung von Individualverfahren auf Antrag, die Führung amtswegiger Verfahren, die Führung internationaler, grenzüberschreitender Verfahren, die Akkreditierung von Verhaltensregeln, die Bearbeitung von Data Breach Meldungen, die Verordnungserlassung betreffend ua. die Datenschutz-Folgenabschätzung (blacklist/whitelist) sowie die

Führung von Verwaltungsstrafverfahren. Die Datenschutzbehörde ist darüber hinaus als aktives Mitglied in zahlreichen internationalen und nationalen Gremien präsent.

Die Arbeit der Datenschutzbehörde war im Jahr 2019 geprägt von der Datenschutz-Grundverordnung und den ersten Verfahren die inhaltlich nach den neuen Normen zu entscheiden waren. In vielen Fällen wurde – nicht nur von den Verantwortlichen und Auftragsverarbeitern, sondern auch von der Datenschutzbehörde juristisches Neuland betreten.

Die Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörde haben im Jahr 2019 sowohl national als auch international unzählige Vorträge gehalten, viele Veranstaltungen und Konferenzen im Bereich des Datenschutzes besucht.

Die Wichtigkeit des Grundrechts auf Datenschutz wird durch die DSGVO unterstrichen und die Aufgabe der europäischen Datenschutzbehörden ist es nunmehr, die einheitliche Anwendung der Verordnung in der europäischen Union zu gewährleisten.

An dieser Stelle sei festgehalten, dass die Datenschutzbehörde im Jahr 2019 keine zusätzlichen A1 Planstellen erhalten hat. Die Anzahl von 33,9 Vollzeitäquivalenten hält mit der Vervielfachung (siehe Bericht) des Beschwerdeanfalls und der zusätzlichen Tätigkeiten, die die Behörde seit 25. Mai 2018 wahrzunehmen hat, nicht mit.

Aus diesem Grund wurde nicht nur bereits im Jahr 2018 ein weiterer Antrag zur Personalaufstockung im A1 und A2-Bereich gestellt, der im Jahr 2019 und zu Jahresbeginn 2020 erneuert wurde, sondern auch dem Datenschutzrat und dem jeweiligen Bundesminister in persönlichen Gesprächen der Personalbedarf der Behörde immer wieder kundgetan.

Ich gehe nach wie vor davon aus, dass die Republik Österreich die Datenschutzbehörde mit jenem Personal (Art. 52 DSGVO) ausstatten wird, damit diese ihren Verpflichtungen, die ihr aus dem DSG und der DSGVO erwachsen, nachkommen kann.

Der Datenschutzbericht 2019 ist der sechste, gemäß § 23 Abs. 1 DSG (iVm Art. 59 DSGVO), jährlich zu erstellende Bericht über die Tätigkeit der Datenschutzbehörde, der der Bundesministerin für Justiz bis 31. März des Folgejahres zu übergeben und in geeigneter Weise durch die Behörde zu veröffentlichen ist. Die Veröffentlichung wird auf der Website der Datenschutzbehörde erfolgen.

Interessierte können sich auch während des Jahres über die Tätigkeiten der Datenschutzbehörde informieren; der seit 01./2015 quartalsmäßig erscheinende Newsletter der DSB gibt einen guten Überblick über Neuerungen, Judikatur und sonstige interessante Bereiche aus der nationalen und internationalen Welt des Datenschutzes.

Die Datenschutzbehörde stellt einen Leitfaden zur DSGVO auf ihrer Website zur Verfügung, der regelmäßig aktualisiert wird. Die jüngste Aktualisierung erfolgte im Jänner 2020.

Dr. Andrea Jelinek

Leiterin der Datenschutzbehörde

2 Die Datenschutzbehörde

2.1 Organisation und Aufgaben

2.1.1 Die Datenschutzbehörde

Die Datenschutzbehörde ist monokratisch strukturiert, aufgrund europarechtlicher und völkerrechtlicher Vorgaben unabhängig und keiner Dienst- und Fachaufsicht unterworfen.

Die Leiterin der Datenschutzbehörde ist Dr. Andrea Jelinek, der stellvertretende Leiter Dr. Matthias Schmidl. Beide wurden vom Bundespräsidenten auf Vorschlag der Bundesregierung mit 1. Jänner 2014 für die Dauer von fünf Jahren bestellt und mit Entschließung des Bundespräsidenten vom 20. Dezember 2018 für weitere fünf Jahre wiederbestellt.

2.1.2 Aufgaben und Befugnisse

- Beschwerdeverfahren (Art. 77 DSGVO iVm § 24 DSG)
- Amtswegige Prüfverfahren (Art. 57 Abs. 1 lit. h DSGVO)
- Verfahren betreffend die Datenverarbeitung für Zwecke der wissenschaftlichen Forschung und Statistik (§ 7 DSG) sowie die Datenverarbeitung von Adresdaten zur Benachrichtigung und Befragung von betroffenen Personen (§ 8 DSG)
- die Erlassung von Standardvertragsklauseln zur Heranziehung von Auftragsverarbeitern (Art. 28 DSGVO) unter Einbindung des Europäischen Datenschutzausschusses
- die Entgegennahme und Prüfung von Meldungen über die Verletzung des Schutzes personenbezogener Daten nach Art. 33 DSGVO sowie die Anordnung von Abhilfemaßnahmen
- die Erlassung von Verordnungen betreffend die (Nicht-)Durchführung einer Datenschutz-Folgenabschätzung unter Einbindung des Europäischen Datenschutzausschusses
- die Führung von Konsultationsverfahren nach Art. 36 DSGVO
- die Entgegennahme von Meldungen über die Bestellung von Datenschutzbeauftragten (Art. 37 Abs. 7 DSGVO)
- die Prüfung und Genehmigung von eingereichten Verhaltensregeln (Art. 40 DSGVO) sowie die Erlassung der korrespondierenden Verordnung über die Akkreditierung von Überwachungsstellen (Art. 41 DSGVO) unter Einbindung des Europäischen Datenschutzausschusses
- Genehmigung von Zertifizierungskriterien (Art. 42 DSGVO) sowie die Erlassung der korrespondierenden Verordnung über die Akkreditierung von Zertifizierungsstellen (Art. 43 DSGVO) unter Einbindung des Europäischen Datenschutzausschusses
- Die Genehmigung von verbindlichen internen Vorschriften (BCR) sowie von Vertragsklauseln zur Übermittlung von Daten an Empfänger in Drittstaaten oder internationalen Organisationen (Art. 46 f DSGVO) unter Einbindung des Europäischen Datenschutzausschusses
- die Führung von Verwaltungsstrafverfahren (Art. 83 DSGVO iVm § 62 DSG)
- die strukturierte Zusammenarbeit mit anderen Aufsichtsbehörden bei grenzüberschreitenden Fällen (Art. 60 f DSGVO)
- die Mitarbeit im Europäischen Datenschutzausschuss (Art. 63 ff DSGVO)

Art. 58 DSGVO sieht weitgehende Befugnisse der Aufsichtsbehörden vor. Zu erwähnen sind hier insbesondere

- die Befugnis im Falle einer festgestellten Verletzung der DSGVO Abhilfemaßnahmen anzuordnen, um die Rechtsverletzung abzustellen sowie
- die Befugnis substantielle Geldbußen bei Verstößen gegen die DSGVO zu verhängen, und zwar zusätzlich zu oder anstelle einer sonstigen Abhilfemaßnahme.

Alle Bescheide der Datenschutzbehörde, deren Anzahl sich aufgrund der zusätzlichen Aufgabengebiete vervielfacht hat, können mit Beschwerde an das Bundesverwaltungsgericht bekämpft werden. Dieses entscheidet im Dreiersenat (ein Berufsrichter, zwei Laienrichter). Entscheidungen des Bundesverwaltungsgerichtes können – auch von der Datenschutzbehörde – mit Revision an den Verwaltungsgerichtshof bzw. Beschwerde an den Verfassungsgerichtshof bekämpft werden.

Die Datenschutzbehörde stellt auf der Website der DSB allgemeine Informationen zu den Verfahren vor der Datenschutzbehörde sowie Musterformulare für Eingaben zur Verfügung.

Die Entscheidungen der Datenschutzbehörde werden nur dann im RIS veröffentlicht, wenn sie von der Rechtsprechung der Datenschutzkommission bis 31.12.2013 abweichen, es keine Rechtsprechung der Datenschutzkommission zu einer Rechtsfrage gibt, diese Rechtsprechung uneinheitlich ist oder es sich um eine Entscheidung handelt, die aufgrund der DSGVO getroffen wird und einen bis dato noch nicht judizierten Bereich betrifft. Die Veröffentlichung erfolgt grundsätzlich dann, wenn keine Anfechtung vor dem Bundesverwaltungsgericht erfolgt.

2.2 Der Personalstand

Im Berichtszeitraum versahen am Jahresende 2019 36 Personen in Teil- oder Vollzeit ihren Dienst bei der Datenschutzbehörde, davon 23 Juristinnen und Juristen (davon vier Praktikanten), 4 Mitarbeiterinnen im gehobenen Dienst und 9 Mitarbeiterinnen und Mitarbeiter im Fachdienst. Die Bediensteten der Datenschutzbehörde sind in Erfüllung ihrer Aufgaben an die Weisungen der Leitung gebunden.

Die Vervielfachung der Beschwerden (siehe auch Punkt 5 des Berichts) führte nicht nur zu einer sehr hohen Arbeitsbelastung, die Verfahrensführung dieser nationalen und internationalen Beschwerden bedingen großes Fachwissen. Flexibles switchen zwischen Deutsch und Englisch als Arbeitssprachen ist erforderlich. Die Vielzahl der Data Breach Notifications sowie die Führung der Verwaltungsstrafverfahren zeigen deutlich, dass die Datenschutzbehörde auch 2020 zusätzlichen Personalbedarf hat.

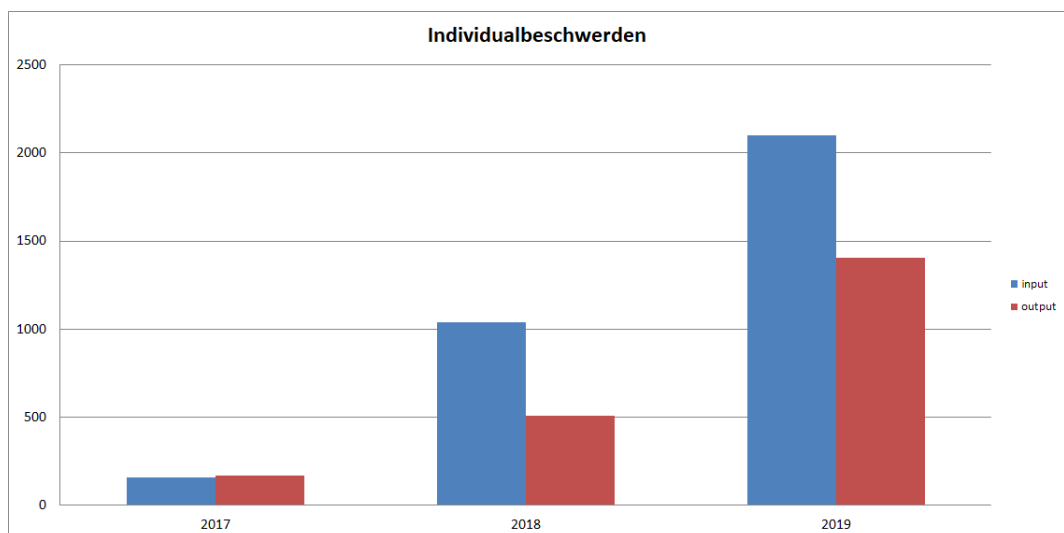
3 Tätigkeit der Datenschutzbehörde

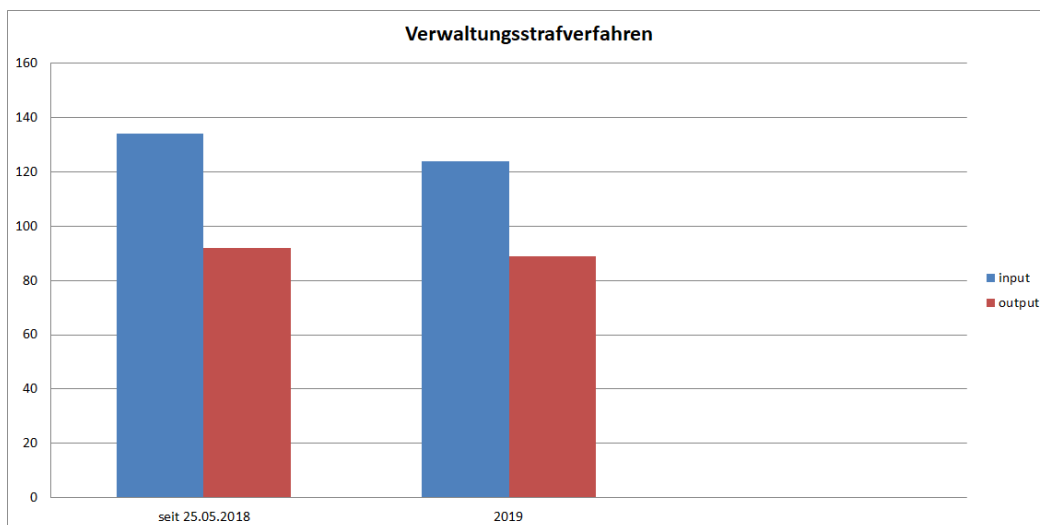
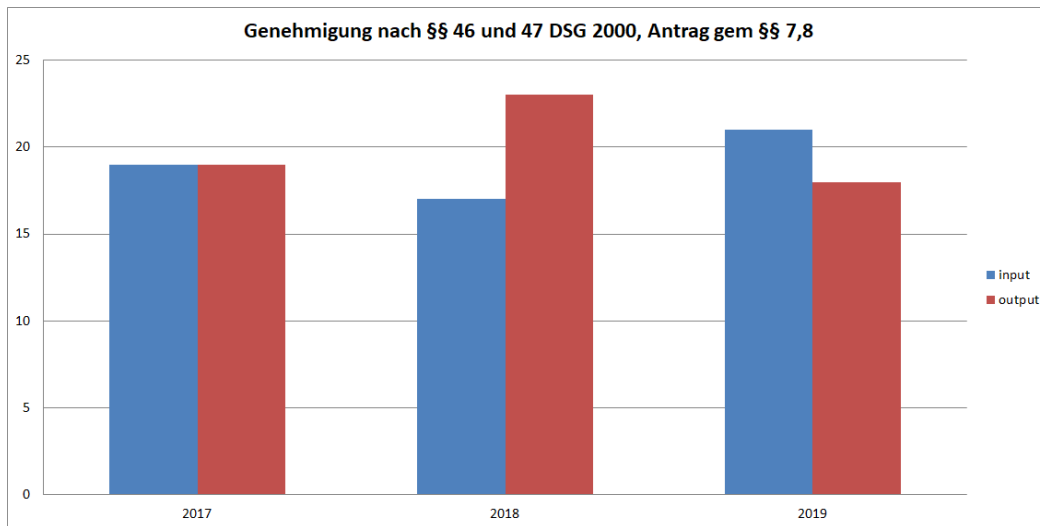
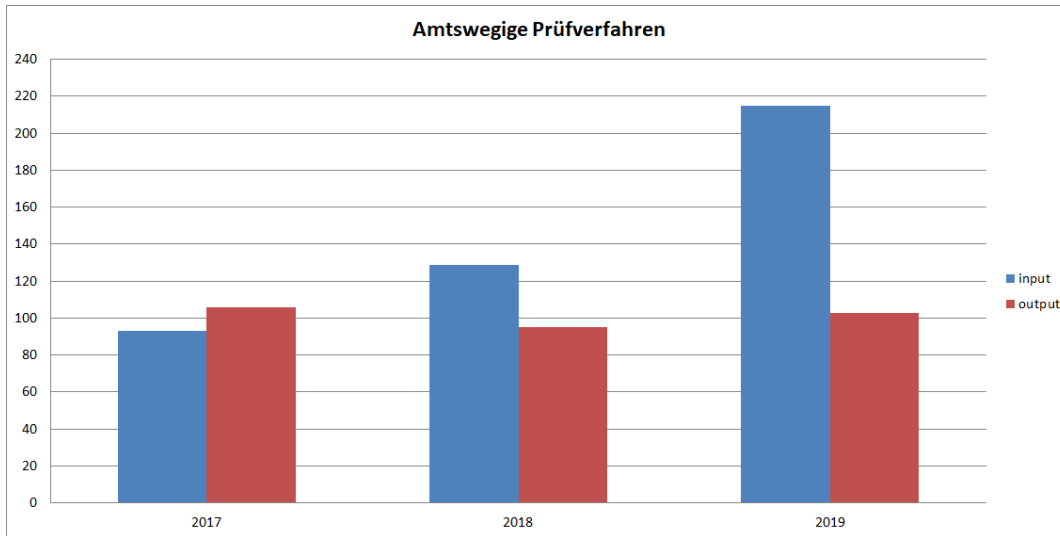
3.1 Statistische Darstellung

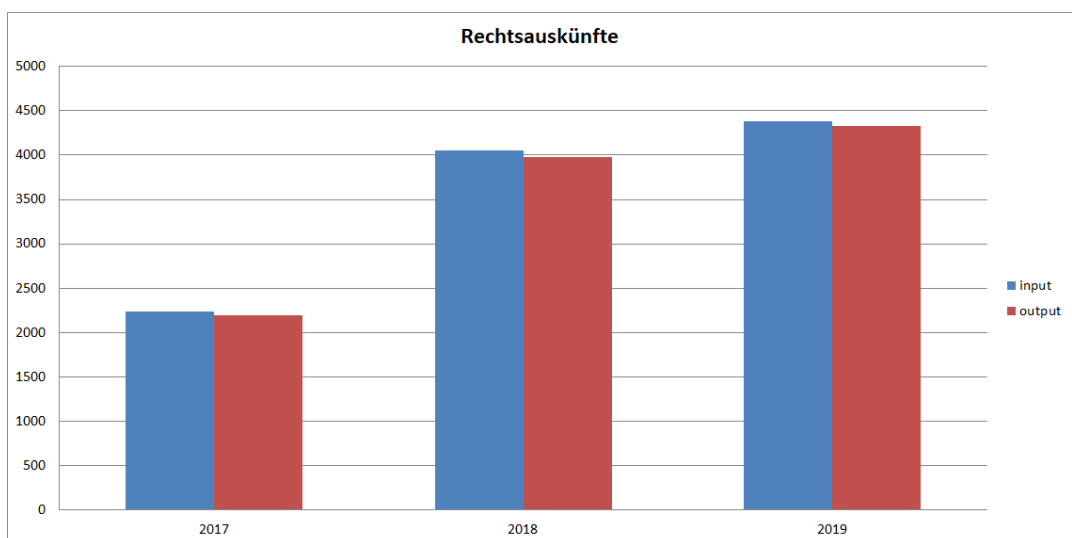
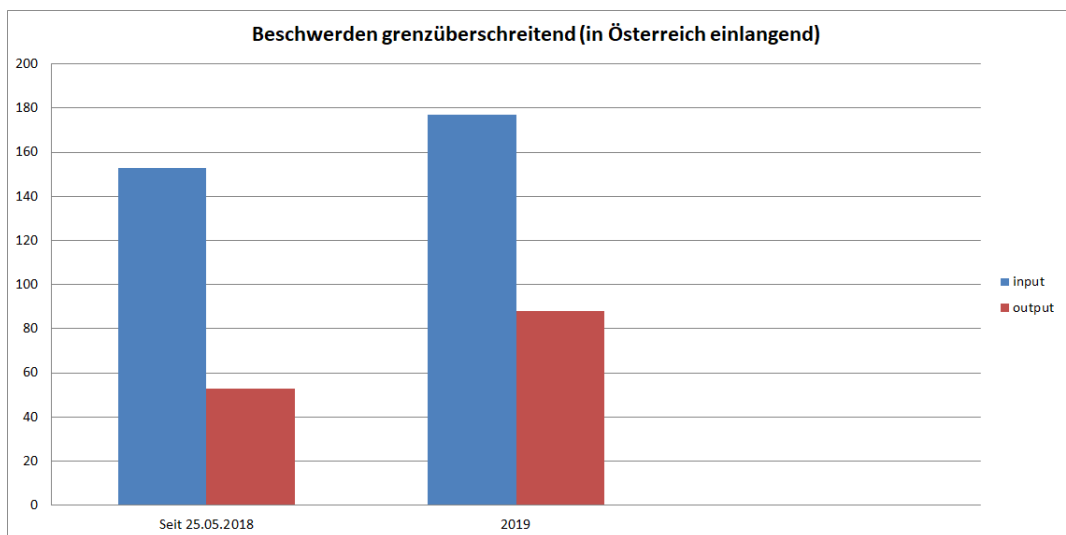
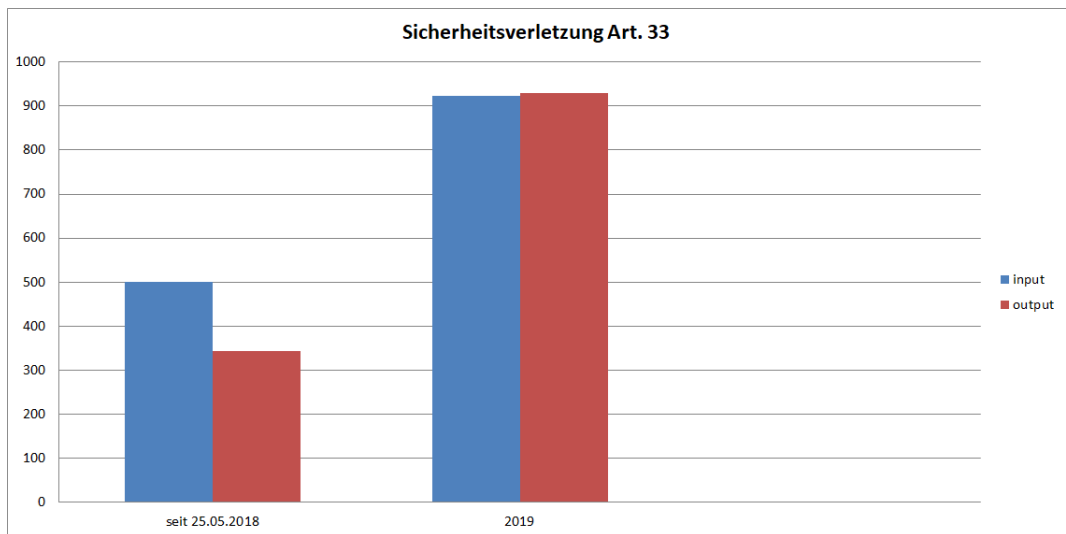
Tabelle 1 Anzahl der Eingangsstücke und Erledigungen

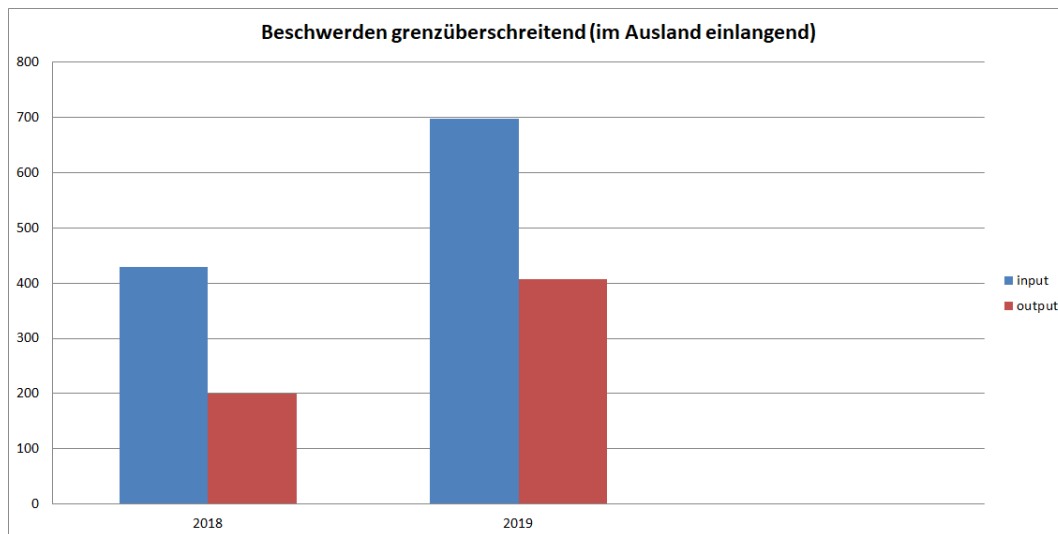
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2017	2018	2019	2017	2018	2019
Individualbeschwerden	156	1036	2102	170	509	1405
Erledigungsart der Individualbeschwerden				115 Bescheide	340 Bescheide	828 Bescheide
				55 Einstellungen	169 Einstellungen	577 Einstellungen
Beschwerden Grenzüberschreitend seit 25.05.2018 (im Ausland einlan- gend)		430	698		200	407
Beschwerden Grenzüberschreitend seit 25.05.2018 (in Österreich einlan- gend)		153	177		53	88
Amtswegige Prüfverfahren	93	129	215	106	95	103
Genehmigungen nach §§ 46 und 47 DSG 2000 (wissenschaftliche Forschung u. Statistik) Antrag gem. §§ 7,8	19	17	21	19	23	18
Genehmigungen im Internationa- len Datenverkehr	185	27	1	201	119	1
Auskunft Schengen	15	19	114	15	16	104
Verwaltungsstrafverfahren seit 25.05.2018		134	124		92	89
Standardvertragsklauseln seit 25.05.2018		1	2		0	1
Verfahren vor dem Bundesverwal- tungsgericht	33	50	164			
Sicherheitsverletzungen § 95a		69	44		77	44
Sicherheitsverletzungen Art 33 seit 25.05.2018		501	923		344	929
Sicherheitsverletzungen grenz- überschreitend seit 25.05.2018 (in Österreich eingelangend)		7	11		4	14

Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2017	2018	2019	2017	2018	2019
Sicherheitsverletzungen grenzüberschreitend seit 25.05.2018 (im Ausland einlangend)		43	71		8	41
Rechtsauskünfte	2239	4052	4384	2192	3974	4329
Amtshilfeersuchen Ausland		13	40		5	33
Anträge auf Genehmigung von Verhaltensregeln seit 25.05.2018		8	6		1	8
Genehmigung BCR (International)		60	20		60	20
Konsultationsverfahren seit 25.05.2018		2	5		2	3
Datenschutzbeauftragte	35	4754	922	35	4754	922
Verkehr mit Behörden		226	163		226	163









3.2 Verfahren und Auskünfte

3.2.1.1 Individualbeschwerden Inland

Allgemeines und Grundsätzliches

Das Beschwerdeverfahren nach § 24 DSOG iVm Art. 77 DSGVO ist das wichtigste Rechtsschutzverfahren zur Durchsetzung von Betroffenenrechten.

Es handelt es sich dabei um ein Zwei- oder Mehrparteienverfahren, in dem die Seiten gegensätzliche Standpunkte vertreten (= kontradiktorisches Verfahren). Die Parteien werden als Beschwerdeführer und Beschwerdegegner bezeichnet.

In diesem Abschnitt werden Verfahren ohne Auslandsbezug behandelt. Das sind Beschwerden, die bei der Datenschutzbehörde eingebracht worden sind, und bei denen der Beschwerdegegner (regelmäßig der für die Verarbeitung Verantwortliche) seine Hauptniederlassung in Österreich hat oder Daten ausschließlich für Zwecke einer inländischen Niederlassung des Beschwerdegegners verarbeitet worden sind.

Internationale Verfahren (einschließlich solcher, bei denen Kapitel VII der DSGVO zur Anwendung gekommen ist) werden im folgenden Abschnitt behandelt.

Die nationale Begleitgesetzgebung zur DSGVO hat in § 24 DSOG das Beschwerderecht verfahrensrechtlich als Recht auf ein förmliches Rechtsschutzverfahren ausgestaltet, in dem die Datenschutzbehörde gerichtsähnlich, streitentscheidend und daher unparteiisch tätig wird. Dem Beschwerdeführer wird dabei mehr abverlangt als das Verfassen eines kurzen und formlosen Beschwerdeschreibens. Bedingt ist dies durch die verfahrensrechtliche Vorgabe, dass ein abgrenzbarer Sachverhalt mit möglichst genau feststehenden Beteiligten (eine „Verwaltungssache“ im Sinne des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG) dargelegt werden muss, den die Datenschutzbehörde zu untersuchen und rechtlich zu beurteilen hat. Die Datenschutzbehörde hat zur Erleichterung dieser Anforderungen u.a. verschiedene Formulare auf ihrer Website zur Verfügung gestellt, deren Verwendung sicherstellen soll, dass eine Beschwerde nicht an verfahrensrechtlichen Formalitäten scheitert. Die Form- und Inhaltserfordernisse des § 24 Abs. 2 und 3 DSOG werden streng gehandhabt. Wer entsprechende Mängel (etwa das

Fehlen des Nachweises eines gestellten Antrags auf Auskunft oder Löschung) nicht binnen einer gesetzten Frist beheben kann, muss mit der Zurückweisung seiner Beschwerde rechnen.

Die zweisprachige Gestaltung mehrerer Formulare (deutsch mit englischer Übersetzung) ermöglicht deren Verwendung in den Verfahren gemäß Kapitel VII DSGVO, da dort Englisch als Arbeitssprache verwendet wird. Die Beschwerde ist jedoch auf Deutsch einzubringen (Art. 8 B-VG).

Auf barrierefreie Gestaltung und die Möglichkeit zur Anbringung einer elektronischen Signatur wurde bei der Gestaltung der Formulare Rücksicht genommen.

Die Reichweite der inländischen Zuständigkeit der Datenschutzbehörde kann derzeit so beschrieben werden:

Die Datenschutzbehörde ist im Inland für Beschwerden gegen alle Rechtsträger öffentlichen und privaten Rechts zuständig, die personenbezogene Daten verarbeiten, ausgenommen sind die folgenden Gebiete:

- die Gesetzgebung von Bund und Ländern (samt zugeordneten Prüfororganen wie Rechnungshof und Volksanwaltschaft),
- die Gerichtsbarkeit, soweit sie justizielle Aufgaben (einschließlich Angelegenheiten der Justizverwaltung, die durch Richterkollegien entschieden werden, Art. 87 Abs. 2 B-VG) wahrnimmt,
- Datenverarbeitungen, die durch natürliche Personen ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten vorgenommen werden, und
- Datenverarbeitungen für Zwecke der Medienberichterstattung.

Fragen hinsichtlich der Zuständigkeit der Datenschutzbehörde für Beschwerden im Bereich der Justizbehörden, insbesondere der Staatsanwaltschaften, sind inzwischen weitgehend durch die Verwaltungsgerichte geklärt. Die Datenverarbeitung durch die Staatsanwaltschaften unterliegt der Kontrolle durch die Datenschutzbehörde.

Beim Beschwerdeverfahren handelt es sich um ein Verwaltungsverfahren nach dem AVG. Es wird getrennt von einem eventuell anschließenden Verwaltungsstrafverfahren geführt. Es handelt sich daher gewissermaßen um die zivilrechtliche Seite der Tätigkeit einer Aufsichtsbehörde für Datenschutz. Im Beschwerdeverfahren besteht gemäß Art. 31 DSGVO für Verantwortliche und Auftragsverarbeiter eine – durch Geldbußen sanktionierbare – Pflicht, mit der Datenschutzbehörde zusammenzuarbeiten.

Auf Grund der Ergebnisse des Beschwerdeverfahrens, einbeziehend das Verhalten des Beschwerdegegners, wird regelmäßig entschieden, ob auch die Einleitung eines Verwaltungsstrafverfahrens erforderlich ist (siehe Abschnitt 3.2.1).

Gemäß Art. 80 Abs. 1 DSGVO können sich betroffene Personen vor der Datenschutzbehörde durch Organisationen ohne Gewinnerzielungsabsicht vertreten lassen, die Datenschutz als satzungsmäßigen Zweck verfolgen. Das in Art. 80 Abs. 2 DSGVO als Option vorgesehene Recht solcher Organisationen, auch ohne Auftrag und Vollmacht Betroffener Beschwerden einzubringen (Verbandsbeschwerde), ist in Österreich nicht vorgesehen. Es besteht vor der Datenschutzbehörde (und vor dem als Rechtsmittelinstanz fungierenden Bundesverwaltungsgericht) für keine Verfahrenspartei eine Pflicht, sich durch einen berufsmäßigen Parteienvertreter vertreten zu lassen.

Der Datenschutzbehörde kommt von Gesetzes wegen im Beschwerdeverfahren die Rolle einer unabhängigen Streitentscheidungsinstanz zu (Art. 57 Abs. 1 lit. f und Art. 77 DSGVO, § 24 Abs. 1 und Abs. 5, § 32 Abs. 1 Z 4 DSG). Die Entscheidungen im Verfahren werden durch die Leiterin der DSB oder in ihrem Namen durch ihren Stellvertreter oder einen aufgrund einer Ermächtigung handelnden Vertreter getroffen. Die ermächtigten Vertreter sind an allfällige Weisungen der Leiterin gebunden.

Im Verfahren wegen Verletzung der Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Unterlassung automatisierter Einzelfallentscheidungen nach der DSGVO muss dem Beschwerdeverfahren vor der Datenschutzbehörde zwingend ein „Vorverfahren“ zwischen der betroffenen Person und dem Verantwortlichen vorangegangen sein, in dem Erstere das jeweilige Recht geltend gemacht hat. Die Ausübung des Rechts muss der Datenschutzbehörde bei Beschwerdeerhebung nachgewiesen werden (§ 24 Abs. 3 DSG).

Das Verfahren zur Durchsetzung der Rechte der betroffenen Person bei der Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs (3. Hauptstück des DSG, keine Anwendung der DSGVO) ist in etwas stärkerem Maß durch die Möglichkeit der Datenschutzbehörde geprägt, als Aufsichtsbehörde nicht nur streitentscheidend tätig zu werden, sondern auch im Interesse der betroffenen Person aktiv in das Verfahren einzugreifen („kommissarischer Rechtsschutz“, vgl. insbesondere § 42 Abs. 8 und 9 DSG).

Praxis der Beschwerdeverfahren im Jahr 2019

Das Berichtsjahr war durch das seit dem Wirksamwerden der DSGVO zu beobachtende starke Ansteigen der Zahl der eingebrachten Beschwerden gekennzeichnet. Details enthält das Kapitel Statistik (Abschnitt 3.1).

Im Berichtsjahr konzentrierten sich die Beschwerdeverfahren auf die Rechte auf Auskunft, Geheimhaltung, Berichtigung/Löschung und Widerspruch. Das in § 1 DSG normierte nationale Grundrecht auf Geheimhaltung bildet in der Praxis dabei den Rahmen, innerhalb dessen die „Grundsätze“ gemäß Kapitel II der DSGVO wie ausdrückliche Betroffenenrechte gemäß Kapitel III der DSGVO geltend gemacht werden können. Die in Kapitel III der DSGVO geregelten Rechte auf Einschränkung (Art. 18 DSGVO), Datenübertragbarkeit (Art. 20 DSGVO) und Unterlassung automatisierter Einzelfallentscheidungen (Art. 22 DSGVO) waren im Berichtszeitraum kein Gegenstand berichtenswerter Entscheidungen.

Das nationale Grundrecht auf Geheimhaltung kann weiterhin auch von juristischen Personen (etwa einer Gesellschaft m.b.H.) durch Beschwerde geltend gemacht werden. Hier bestehen allerdings einige Fragestellungen, da die österreichische Anpassungsgesetzgebung zur DSGVO zwar das nationale Datenschutz-Grundrecht unverändert gelassen hat, die neuen einfachgesetzlichen und verfahrensrechtlichen Regelungen (vgl. § 4 Abs. 1 DSG) aber klar auf den Rechtsschutz natürlicher Personen zugeschnitten wurden. Eine grenzüberschreitende Geltendmachung des Grundrechts durch juristische Personen in Verfahren nach Kapitel VII DSGVO ist wohl auf die von EuGH (Urteil vom 9.11.2010, C-92/09 und C-93/09, Schecke und Eiffert) aufgestellten Kriterien (Name einer natürlichen Person als Namensbestandteil) beschränkt. Ebenfalls nicht (denk-) möglich ist eine Verletzung des Geheimhaltungsrechts juristischer Personen durch eine Video-

überwachung (siehe Bescheid vom 13.9.2018, GZ: DSB-D216.713/0006-DSB/2018, RIS, Datenschutzbericht 2018, Seite 66).

Die verfahrensgesetzlich geregelte Möglichkeit, Beschwerdeverfahren als „gegenstandslos“ durch Einstellung zu beenden (§ 24 Abs. 6 DSG) ermöglicht es, insbesondere Beschwerdeverfahren wegen Auskunfts- oder Löschungsanträgen, auf die der Verantwortliche in gesetzwidriger Weise zunächst nicht reagiert hat, nach Erreichung des primären Verfahrensziels (Beantwortung des Auskunfts- oder Löschungsantrags) ohne großen Aufwand zu beenden. Eine solche Einstellung des Beschwerdeverfahrens schützt den Verantwortlichen jedoch nicht vor möglichen verwaltungsstrafrechtlichen Folgen.

Im Berichtszeitraum hat die Datenschutzbehörde erstmals mehrfach von der Möglichkeit Gebrauch gemacht, die Behandlung von Beschwerden gemäß Art. 57 Abs. 4 DSGVO wegen exzessiver Nutzung des Beschwerderechts abzulehnen. Eine einzelne Person hatte dabei im Berichtsjahr allein fast 100 Beschwerden (rein inländische wie internationale) eingebracht, die sich alle in mehr oder weniger deutlicher Ausprägung um denselben Sachverhaltskomplex drehten. Alle diese bisherigen Ablehnungsbescheide sind beim Bundesverwaltungsgericht angefochten worden.

Ausgewählte Beschwerdeentscheidungen aus 2019

Die DSB hat in ihrer öffentlich zugänglichen Entscheidungsdokumentation (im Rahmen des Rechtsinformationssystems des Bundes – RIS; Stand: 6. Februar 2020) aus dem Jahr 2019 29 Bescheide aus inländischen Beschwerdeverfahren dokumentiert. Diese Zahl kann sich aus verschiedenen Gründen (z.B. wegen abzuwartender Rechtsmittelentscheidungen des BVwG, VfGH oder VwGH) nach Erscheinen des Datenschutzberichts 2019 ändern.

Regelmäßig werden rechtskräftige Entscheidungen dokumentiert, Ausnahmefälle sind in den RIS-Dokumenten durch entsprechende Vermerke gekennzeichnet. In solchen Fällen wird die Entscheidung nach einer Aufhebung durch das Bundesverwaltungsgericht aus dem RIS entfernt oder der sonstige Ausgang des Verfahrens dokumentiert. Nicht alle im RIS dokumentierten Entscheidungen scheinen in der nachfolgenden Übersicht auf.

Über andere, insbesondere nicht rechtskräftige Entscheidungen, wird mehrfach pro Jahr im Newsletter der Datenschutzbehörde berichtet.

Die wichtigsten Beschwerdeentscheidungen in chronologischer Reihenfolge:

1. Bescheid vom 2.1.2019, GZ: DSB-D123.627/0003-DSB/2018 (Einwilligung, als Beschwerdegegner bezeichneter Verantwortlicher, rechtskräftig, RIS)

Der Beschwerdeführer brachte (ausdrücklich und nach einem Mangelbehebungsauftrag) gegen einen in den Niederlanden niedergelassenen Verantwortlichen Beschwerde wegen Verletzung des Auskunftsrechts und wegen „Rechtmäßigkeit der Einwilligung“ ein. Außerdem verletze die Website des Unternehmens die Bestimmungen über die Informationspflichten. Er sei entgegen der DSGVO informiert worden, dass er dem Erhalt von E-Mail-Werbung innerhalb gewisser Frist widersprechen müsse. Ein Antrag auf Auskunft wurde nicht vorgelegt, aus der vorgelegten Korrespondenz ging zweifelsfrei hervor, dass die Daten für Zwecke eines im Vereinigten Königreich niedergelassenen Unternehmens verarbeitet werden, das auch für die bezeichnete Website verantwortlich ist.

Hinsichtlich der „Rechtmäßigkeit der Einwilligung“ führte die Datenschutzbehörde aus, dass in Art. 7 DSGVO lediglich gewisse Voraussetzungen, die einen Rechtfertigungsgrund zur Da-

tenverarbeitung bilden können, festgelegt sind. Aus der genannten Bestimmung lassen sich per se keine subjektiven Rechte ableiten, weswegen schon nach dem Wortlaut des § 24 Abs. 2 Z. 2 DSGVO die Voraussetzung, dass das als verletzt erachtete Recht bezeichnet werden muss nicht erfüllt ist. Die Beschwerde wurde in diesem Punkt wegen nicht erfolgter Mangelbehebung zurückgewiesen.

Da nach der Rechtsprechung des VwGH eine klar bezeichnete Partei (Beschwerdegegner) nicht ausgetauscht werden darf, und der bezeichnete Beschwerdegegner als Verantwortlicher hinsichtlich weiterer behaupteter Eingriffe in Rechte des Beschwerdeführers nicht in Frage kam, wurde die Beschwerde im Übrigen abgewiesen.

Dieser Bescheid ist rechtskräftig.

2. Bescheid vom 11.1.2019, GZ: DSB-D123.512/0004-DSB/2018 (Einwurf in Briefkasten der Hausbesorgerin kein wirksam gestellter Auskunftsantrag, rechtskräftig, RIS)

In dieser Sache behauptete der Beschwerdeführer, durch Einwurf eines Auskunftsantrags in den Briefkasten der Hausbesorgerin einen – unerfüllt gebliebenen - Antrag auf Auskunftserteilung an die Hausverwaltung gestellt zu haben. Letztere bestritt den Erhalt des Auskunftsverlangens.

Der Beschwerdeführer hat letzteren Einwand nicht bestritten oder widerlegt. Er führte lediglich aus, dass er die Zustellung durch Einwurf in den Briefkasten als rechtlich wirksam erachte. Dieses Argument verneinte die Datenschutzbehörde, da die Entgegennahme und Weiterleitung von Post an die Hausverwaltung nicht zu den gesetzlichen Dienstpflichten eines Hausbesorgers gehört, und die Hausverwaltung für solche Fälle auf ihrer Webseite ein Kontaktformular (vgl. Art. 12 Abs. 1 DSGVO) für datenschutzrechtliche Eingaben bereitgestellt hatte. Das Auskunftsrecht nach Art. 15 DSGVO ist konzeptionell ein antragbedürftiges Recht und bedarf eines dem Verantwortlichen zugegangenen Antrags. Die Beschwerde wurde daher abgewiesen.

Dieser Bescheid ist rechtskräftig.

3. Bescheid vom 15.1.2019, GZ: DSB-D123.527/0004-DSB/2018 (Kein Recht auf Löschung aus einer Arztsuch- und Bewertungsplattform, rechtskräftig, RIS, Newsletter 3/2019, Seite 4)

In diesem Bescheid hatte die Datenschutzbehörde darüber zu entscheiden, ob die Beschwerdegegnerin, die eine Arztsuch- und Bewertungsplattform betreibt, dem Löschbegehren eines Arztes, der die vollständige Löschung all seiner Daten samt Bewertungen und Erfahrungsberichten aus dieser Plattform begehrte, zurecht nicht entsprochen hat.

Die Datenschutzbehörde hielt dabei zunächst fest, dass die Verknüpfung von Daten gemäß § 27 Abs. 1 Z 1 bis 17 ÄrzteG 1998 mit der Möglichkeit der Abgabe einer Bewertung sowie eines Erfahrungsberichts ein (neuer) Verarbeitungsvorgang ist, der einen Erlaubnistatbestand benötigt. Die Beschwerdegegnerin stützte sich diesbezüglich auf berechnete Interessen nach Art. 6 Abs. 1 lit. f DSGVO, weshalb eine Interessenabwägung durchzuführen war. Bei dieser Interessenabwägung war zunächst zu berücksichtigen, dass die Beschwerdegegnerin geeignete Schutzmaßnahmen implementiert hat, sodass sachlich ungerechtfertigte Kommentare gemeldet und Mehrfachbewertungen – soweit technisch möglich – verhindert werden. Der Beschwerdeführer ist den Bewertungen daher nicht schutzlos ausgeliefert, weshalb keine Prangerwirkung erkennbar ist. Darüber hinaus ist die berufliche Tätigkeit der Sozialsphäre zuzuordnen, weshalb von einer geringeren Schutzwürdigkeit auszugehen ist, als wenn Daten betroffen sind, die der „Intim- oder Geheimsphäre“ zuzuordnen sind. Demgegenüber stand das

berechtigte Interesse der Patienten, Informationen über ärztliche Dienstleistungen einzuholen, zumal in Österreich grundsätzlich eine freie Arztwahl besteht. Durch ein Such- und Bewertungsportal, wie das durch die Beschwerdegegnerin betriebene, erhalten Personen, die einander mitunter nicht kennen, gerade erst die Möglichkeit, sich einfach und effizient über ein bestimmtes Thema auszutauschen und können Personen eine solche Plattform als zusätzliche Such- und Informationsquelle betreffend medizinische Versorgung und Gesundheitsleistungen heranziehen.

Vor diesem Hintergrund gelangte die Datenschutzbehörde zu dem Ergebnis, dass die berechtigten Interessen der Portalbenutzer (der Patienten) gegenüber den dargelegten Beeinträchtigungen der berechtigten Interessen des Beschwerdeführers überwiegen, weshalb die Beschwerdegegnerin dem Löschbegehren zurecht nicht entsprochen hat und die Beschwerde daher abgewiesen wurde.

Dieser Bescheid ist rechtskräftig.

4. Bescheid vom 22.1.2019, DSB-D123.848/0001-DSB/2019 (Unterhaltsverfahren beim Bezirksgericht justizielle Tätigkeit, Datenschutzbehörde unzuständig, rechtskräftig, RIS)

In diesem Bescheid lag der Datenschutzbehörde eine Beschwerde gegen ein Bezirksgericht wegen Verletzung des Geheimhaltungsrechts in Folge Ermittlung von Einkommensdaten im Verfahren zur Unterhaltsfestsetzung für ein minderjähriges Kind gemäß Außerstreitgesetz (AußStrG) vor.

Die Datenschutzbehörde kam zu dem Schluss, dass es sich bei einem Verfahren betreffend Unterhalt – selbst wenn es sich verfahrensrechtlich nach dem AußStrG richtet – um ein Verfahren handelt, das einen Rechtsstreit beilegen soll und auf eine Entscheidung mit Rechtsprechungscharakter abzielt. Der Beschwerdegegner handelte somit im Rahmen seiner justiziellen Tätigkeit. Die Datenschutzbehörde war daher gemäß Art. 55 Abs. 3 DSGVO zur Behandlung der Beschwerde unzuständig. Die Beschwerde wurde zurück- und der Beschwerdeführer auf das Verfahren nach §§ 83 ff GOG (justizielle Datenschutzbeschwerde) verwiesen.

Dieser Bescheid ist rechtskräftig.

5. Bescheid vom 5.2.2019, DSB-D123.495/0007-DSB/2018 (Inhalt einer Parteierklärung, Datenverarbeitung für Werbezwecke, fehlende Einwilligung, Wegfall der Beschwer im laufenden Verfahren, rechtskräftig, RIS)

In dieser Sache lag der Datenschutzbehörde eine Beschwerde gegen einen Reiseveranstalter vor, der die Daten des Beschwerdeführers, der an einer Reise teilgenommen aber nie eine entsprechende Einwilligung gegeben hatte, für Werbezwecke verarbeitete (E-Mail-Werbung, Katalogversand). Der Beschwerdeführer hatte, zunächst erfolglos, die vollständige Löschung seiner Daten verlangt. Erst im laufenden Beschwerdeverfahren wurden die Daten für Werbezwecke gesperrt (wenn auch nicht vollständig gelöscht).

Zunächst interpretierte die Datenschutzbehörde den Inhalt des Beschwerdebegehrens (formal war eine Verletzung im Geheimhaltungsrecht geltend gemacht worden) so, dass der Beschwerdeführer eine Löschung seiner Daten bzw. die Nichtverarbeitung für Werbezwecke anstrebte. Durch die im laufenden Verfahren abgegebene Erklärung, die Daten des Beschwerdeführers für Werbezwecke zu sperren, sei diesbezüglich die Beschwer weggefallen. Ein Recht auf Feststellung, zeitweilig im Recht auf Löschung verletzt gewesen zu sein, bestehe nicht. Daher wurde die Beschwerde letztlich abgewiesen.

Dieser Bescheid ist rechtskräftig.

6. Bescheid vom 11.2.2019, DSB-D123.463/0005-DSB/2018 (Minderjährigkeit im datenschutzrechtlichen Verfahren, rechtskräftig, Newsletter 2/2019, Seite 3 f)

In diesem Bescheid hatte sich die Datenschutzbehörde aufgrund der Minderjährigkeit des Beschwerdeführers mit dessen Prozessfähigkeit im datenschutzrechtlichen Verfahren auseinander zu setzen. Die Datenschutzbehörde kam zu dem Schluss, dass der Beschwerdeführer zwar aufgrund seines Alters beschränkt prozessfähig (§ 170 Abs. 2 ABGB) ist; diese Prozessfähigkeit aber auf Verfahren, die sich auf die diesem zur freien Verfügung überlassenen Sachen beziehen oder Einkommen aus eigenem Erwerb betreffen - dh. auf vermögensrechtliche Angelegenheiten - beschränkt ist. Die Prozessfähigkeit zur Führung eines datenschutzrechtlichen Verfahrens vor der Datenschutzbehörde kommt dem Beschwerdeführer jedoch nicht zu. In der Sache wurde die Beschwerdeführung zwar nachträglich durch den obsorgeberechtigten Vater genehmigt; der an den Beschwerdeführer zu Händen seines Vaters gerichtete Mangelbehebungsauftrag wurde jedoch nur vom Beschwerdeführer selbst beantwortet. Da der minderjährige Beschwerdeführer nicht prozessfähig ist und damit eigene Willenserklärungen gegenüber der Behörde keine Rechtsfolgen auslösen, wurde dem Mangelbehebungsauftrag der Datenschutzbehörde nicht entsprochen, weshalb die Beschwerde gemäß § 13 Abs. 3 AVG zurückzuweisen war.

Dieser Bescheid ist rechtskräftig.

7. Bescheid vom 20.2.2019, GZ: DSB-D123.319/0002-DSB/2019 (Löschung, Bonitätsdaten, Wirtschaftsauskunftei, Faktoren bei Interessenabwägung, rechtskräftig, RIS)

Der Beschwerdeführer wurde Anfang 2017 in einem Insolvenzverfahren nach Erfüllung eines Zahlungsplans von seinen Schulden befreit. Nunmehr hatte er bei einer Wirtschaftsauskunftei (Beschwerdegegnerin) die Löschung von bonitätsrelevanten Daten verlangt, (insbesondere Daten zum durchgeführten Insolvenzverfahren und den Beschwerdeführer betreffende Eintragungen in einem von der Beschwerdegegnerin geführten Register von Verbraucherkrediten (V***-Evidenz). Dies wurde abgelehnt. Der Beschwerdeführer wandte sich daraufhin wegen behaupteter Verletzung seines Löschungsrechts an die Datenschutzbehörde. Die Verarbeitung der Daten sei gemäß Art. 17 Abs. 1 lit a DSGVO nicht mehr notwendig. Er sei schuldenfrei, wieder solvent und habe ein regelmäßiges Einkommen.

Die Datenschutzbehörde hielt zunächst fest, dass die Beschwerdegegnerin die Verarbeitung von Daten zur Kreditwürdigkeit grundsätzlich auf ihre Gewerbeberechtigung gemäß § 152 GewO 1994 stützen könne. Im Einzelfall sei jeweils eine Interessenabwägung gemäß Art. 6 Abs. 1 lit f DSGVO vorzunehmen. Für die Beurteilung maßgeblich können dabei u.a. folgende Umstände sein: Höhe und Alter der einzelnen Forderungen, Anzahl der im Wege eines Inkassounternehmens eingetriebenen Forderungen, Zeit, die seit Begleichung einer Forderung verstrichen ist, und die Herkunft der Daten. Im Beschwerdefall ergebe diese Interessenabwägung (insbesondere Passiva im Insolvenzverfahren über € 27.400, getilgter Kredit in Höhe von € 6.900, erst rund 2 Jahre seit Restschuldbefreiung im Insolvenzverfahren vergangen), dass das Interesse der Beschwerdegegnerin an der weiteren Verarbeitung der Daten hier überwiege. Die Beschwerde wurde daher abgewiesen.

Dieser Bescheid ist rechtskräftig.

8. Bescheid vom 21.2.2019, GZ: DSB-D123.311/0003-DSB/2019 (Veranstaltungskreditierung, Informationsrecht und Informationspflicht, Freiwilligkeit einer Einwilligung, rechtskräftig, RIS)

Der Beschwerdeführer wandte sich gegen das Bundeskanzleramt, das während der letzten EU-Ratspräsidentschaft ein Online-Akkreditierungssystem für Rahmenveranstaltungen betrieben hatte, und machte Verletzungen in den Rechten auf Information (Art. 13 DSGVO) und

Geheimhaltung (§ 1 DSG) hinsichtlich seiner Akkreditierung für eine bestimmte Veranstaltung geltend. Die Datenschutzbehörde kam zu dem Schluss, dass der Beschwerdegegner in seiner Datenschutzerklärung der Informationspflicht gemäß Art. 13 Abs. 2 lit. e DSGVO nicht nachgekommen sei, dies jedoch im Zuge des laufenden Beschwerdeverfahrens im Sinne von § 24 Abs. 6 DSG nachgeholt habe (Beseitigung der Beschwer, Klaglosstellung. Die Beschwerde wegen Verletzung im Recht gemäß Art. 13 DSGVO wurde daher abgewiesen.

Hinsichtlich der Verletzung im Recht auf Geheimhaltung hatte sich der Beschwerdegegner als Rechtsgrundlage auf die Einwilligung des Beschwerdeführers zur Verarbeitung seiner Daten berufen. U.a. mangels hinreichender Information gemäß Art. 13 DSGVO wurde diese Einwilligung jedoch für unwirksam befunden, der Beschwerde teilweise Folge gegeben und eine Verletzung im Recht auf Geheimhaltung festgestellt.

Dieser Bescheid ist rechtskräftig.

9. Bescheid vom 7.3.2019, GZ: DSB-D123.154/0004-DSB/2019 (Rechtmäßigkeit der Verarbeitung, Gemeinde, Einsichtnahme in dienstlichen E-Mail-Account, rechtskräftig, RIS)

In diesem Bescheid musste sich die Datenschutzbehörde mit einer Frage der Rechtmäßigkeit der Datenverarbeitung im Bereich des öffentlichen Dienstes (Einsichtnahme in einen E-Mail-Account durch den früheren Dienstgeber) beschäftigen.

Der Beschwerdeführer war Amtsleiter bei einer österreichischen Ortsgemeinde (Beschwerdegegnerin). Sein vertragliches Dienstverhältnis wurde beendet, die dienstliche E-Mail-Adresse gerhard.a***@n***bach.gv.at war anschließend noch monatelang funktionsfähig, der externe Zugang des Beschwerdeführers über das Internet wurde aber gesperrt. Es bestanden bei der Gemeinde keine Funktionspostfächer (wie baubehoerde@n***bach.gv.at), Verfahrensparteien sendeten E-Mails häufig an die Adresse des Beschwerdeführers. Eine vertragliche Regelung über die private Nutzung der dienstlichen E-Mail-Adresse bestand ebenfalls nicht.

Der Beschwerdeführer behauptete eine Verletzung im Recht auf Geheimhaltung in Folge vom Bürgermeister veranlasster Einsichtnahmen in den E-Mail-Account gerhard.a***@n***bach.gv.at.

Die Datenschutzbehörde führte aus, dass es im gegenständlichen Verfahren aufgrund des Zwecks des dienstlichen E-Mail Accounts, der für den Beschwerdeführer betreffend seine ehemalige Tätigkeit als Amtsleiter der Beschwerdegegnerin eingerichtet worden ist, nicht ausgeschlossen war, dass sich im Posteingang und Postausgang E-Mails mit Inhalten, die bei der Beschwerdegegnerin anhängige behördliche Verfahren betreffen und in weiterer Folge demnach für die Feststellung eines relevanten Sachverhalts geeignet sind, befinden. Insgesamt war der Eingriff demgemäß nicht als überschießend zu beurteilen. Die Beschwerde wurde daher abgewiesen.

Dieser Bescheid ist rechtskräftig.

10. Bescheid vom 18.3.2019, GZ: DSB-D123.955/0002-DSB/2019 (Zuständigkeit, kein wirksamer Anknüpfungspunkt in Österreich, kein „forum shopping“, rechtskräftig, RIS)

In diesem Bescheid musste die Datenschutzbehörde eine Frage der internationalen Zuständigkeit gemäß Art. 77 DSGVO lösen.

Der Beschwerdeführer, ein rumänischer Staatsbürger ohne gewöhnlichen Aufenthalt in Österreich, erhob Beschwerde wegen Verletzung seines Lösungsrechts gegen Verantwortliche, die erkennbar nicht in Österreich niedergelassen waren bzw. keine Daten für Zwecke einer österreichischen Niederlassung verarbeitet. Im Kern ging es um die Inhalte von Websites (in Domains mit den Endungen .com, .ro und .md), die Vorwürfe gegen den Beschwerdeführer im Zusammenhang mit seiner beruflichen Tätigkeit als Unternehmensleiter in Moldawien (Republik Moldau) erhoben. Der einzige Bezug betreffend eine etwaige Zuständigkeit der österreichischen Datenschutzbehörde war die Tatsache, dass der Beschwerdeführer die Datenschutzbeschwerde in Österreich und in deutscher Sprache eingebracht hatte. Auf Vorhalt, warum er sich, was u.a. aus Sprachgründen naheliegen würde, nicht an die rumänische Aufsichtsbehörde für Datenschutz gewandt habe, brachte er vor: „Meine Meinung ist, dass die österreichische Datenschutzbehörde das Problem besser als die rumänische Datenschutzbehörde lösen kann. [...]“.

Auch wenn der Wortlaut („insbesondere“) des Art. 77 DSGVO als auch jener des ErwGr. 141 es nahelegen, dass eine Beschwerde bei jeder Aufsichtsbehörde iSd DSGVO eingebracht werden kann, so ist dem entgegenzuhalten, dass es nicht Sinn und Zweck des Art. 77 DSGVO sein kann, Aufsichtsbehörden als zur Einbringung einer Beschwerde als zuständig zu erklären, zu denen keinerlei objektiver Konnex besteht. Ziel der DSGVO ist es, die Ausübung von Rechtsschutzinteressen zu erleichtern, indem es Betroffenen ermöglicht wird, eine Beschwerde bei einer Aufsichtsbehörde einzureichen, zu der ein räumliches und/oder sprachliches Naheverhältnis besteht.

Dennoch kann Art. 77 DSGVO nicht so verstanden werden, als ermögliche er eine völlig freie Behördenwahl („forum shopping“) unter Umgehung von Aufsichtsbehörden, denen gegebenenfalls eine ordnungsgemäße Verfahrensführung nicht zugetraut wird, zu denen aber ein objektiver Konnex im oben beschriebenen Sinn besteht.

Die Beschwerde wurde daher wegen fehlender Zuständigkeit zurückgewiesen.

Dieser Bescheid ist rechtskräftig.

11. Bescheid vom 12.4.2019, GZ: DSB-D123.591/0003-DSB/2019 (Eingriff einer Behörde in das Geheimhaltungsrecht eines Journalisten, rechtskräftig, RIS)

In dieser Sache hatte sich die Datenschutzbehörde mit der Beschwerde eines leitenden Redakteurs einer Wochenzeitung zu befassen. Dieser hatte Verletzung in den Rechten auf Geheimhaltung und Löschung durch das Bundesministerium für Inneres (BMI, Beschwerdegegner) geltend gemacht, weil dieses einen SMS-Wechsel des Beschwerdeführers mit Mitarbeitern des BMI veröffentlicht hatte (auf der Website des BMI sowie durch Verlinkung im Kurznachrichtendienst Twitter). Der Beschwerdeführer hatte auch Maßnahmen nach §§ 22 Abs. 4 und 25 Abs. 1 DSG beantragt. Letzterer Antrag wurde mangels Gefahr im Verzug (Veröffentlichung bereits beendet) ab-, die Beschwerde wegen Verletzung im Lösungsrecht mangels Nachweises eines Antrags auf Löschung der Daten zurückgewiesen.

Hinsichtlich der Verletzung im Recht auf Geheimhaltung war die Beschwerde jedoch erfolgreich. Die Datenschutzbehörde hielt fest, dass der Beschwerdegegner eine gesetzliche Grundlage für sein Vorgehen gebraucht hätte, die nicht bestehe. Eine Datenverarbeitung auf Grundlage berechtigter Interessen nach Art. 6 Abs. 1 lit. f DSGVO sei gemäß Abs. 1 letzter Satz leg.cit. bei Behörden in Erfüllung ihrer Aufgaben nicht zulässig. Soweit das Vorgehen des BMI mit einem Bedarf nach Richtigstellung von Informationen begründet wurde, die der Beschwerdeführer veröffentlicht hatte, hätte der Beschwerdegegner eine medienrechtliche Gegendarstellung gemäß § 9 Abs. 1 MedienG verlangen können.

Dieser Bescheid ist rechtskräftig.

12. Bescheid vom 18.4.2019, GZ: DSB-D122.913/0001-DSB/2019 (Kein Recht auf Auskunft zur Identität eines Anzeigers, rechtskräftig, RIS)

Der Beschwerdeführer war wegen einer behaupteten und im Ermittlungsverfahren nicht bestätigten Verwaltungsübertretung bei einer Bezirksverwaltungsbehörde angezeigt worden. Nach Einstellung des Verwaltungsstrafverfahrens verlangte er von der Behörde, gestützt auf § 26 DSG 2000 bzw. Art. 15 DSGVO, Auskunft zur Identität des (ihm bisher nicht offengelegten) Anzeigers. Nach Ablehnung dieser Auskunftserteilung erhob er Beschwerde bei der Datenschutzbehörde. Diese wurde abgewiesen, und die Datenschutzbehörde hielt fest, dass eine Auskunft gemäß Art. 15 DSGVO - wie schon bisher - auf eigene Daten beschränkt, also auf Daten, die dem Wortlaut des Art. 15 Abs. 1 DSGVO zufolge, „sie [dh. die betroffene Person] betreffende personenbezogene Daten“ sind. Daher besteht grundsätzlich auch weiterhin kein Recht auf Auskunft über die personenbezogenen Daten Dritter, soweit im Einzelfall nicht besondere Gründe dafürsprechen. Diese Auslegung des Auskunftsrechts könne sich nunmehr ausdrücklich auf Art. 15 Abs. 4 DSGVO stützen.

Dieser Bescheid ist rechtskräftig.

13. Bescheid vom 23.4.2019, GZ: DSB-D123.626/0006-DSB/2019 (Einmalige Verwendung von personenbezogenen Daten aus dem Grundbuch zwecks möglicher Akquise von Immobilien, rechtskräftig, RIS, Newsletter 3/2019, Seite 4)

In diesem Bescheid hatte sich die Datenschutzbehörde mit der Frage zu beschäftigen, ob es zulässig ist, personenbezogene Daten aus dem Grundbuch zu erheben und diese in weiterer Folge dazu zu verwenden, um Personen postalisch zwecks möglicher Akquise einer Immobilie zu kontaktieren. Der Beschwerdeführer behauptete nach Erhalt des genannten Schreibens eine Verletzung im Recht auf Geheimhaltung.

Die Datenschutzbehörde sprach zunächst aus, dass es sich um personenbezogene Daten handelt, welche im Grundbuch, einem öffentlichen Register, zugänglich sind. Die ganz generelle Annahme des Nichtvorliegens einer Verletzung schutzwürdiger Geheimhaltungsinteressen für zulässigerweise veröffentlichte Daten ist nach Ansicht der Datenschutzbehörde jedoch nicht mit den Bestimmungen der DSGVO vereinbar. Darüber hinaus beschränkte sich die Beschwerdegegnerin nicht auf die bloße Reproduktion dieser öffentlich zugänglichen Daten, sondern wurde mit diesen Daten ein neues Element verknüpft, nämlich die Verwendung der Daten zur möglichen Akquise von Liegenschaften im Rahmen des Gewerbes als Immobilienreuhänder. Da eine solche Verknüpfung nach stRsp der Datenschutzbehörde stets eines Erlaubnistatbestands bedarf, und sich die Beschwerdegegnerin in diesem Zusammenhang auf berechnete Interessen gestützt hat, war eine Interessenabwägung durchzuführen.

Diesbezüglich ist zunächst festzuhalten, dass aufgrund des Umstands, dass die personenbezogenen Daten des Beschwerdeführers bereits im Grundbuch öffentlich zugänglich sind und es sich dabei offenkundig um keine sensiblen Daten und auch um keine strafrechtlich relevanten Daten handelt, grundsätzlich von einer geringeren Schutzwürdigkeit auszugehen ist. Der Beschwerdeführer wurde lediglich einmal postalisch kontaktiert und die personenbezogenen Daten auch nicht anderweitig verwendet. Die Beschwerdegegnerin hat darüber hinaus als Immobilienreuhänder das Interesse, laufend Liegenschaften bzw. Grundstücke zu erwerben, die aus ihrer Sicht von wirtschaftlichem Interesse sind. Ferner hat die Beschwerdegegnerin auch angeboten, die personenbezogenen Daten des Beschwerdeführers zu löschen bzw. eine weitere Kontaktaufnahme zu unterlassen. Umgekehrt hat der Beschwerdeführer keine schutzwürdigen Geheimhaltungsinteressen ins Treffen geführt und waren diese auch nicht erkennbar. Die Datenschutzbehörde gelangte daher zu dem Ergebnis, dass aufgrund der durchgeführten Interessenabwägung keine Verletzung im Recht auf Geheimhaltung vorliegt, da die berechtigten

Interessen der Beschwerdegegnerin als Immobilitentreuhänder gegenüber den Beeinträchtigungen der berechtigten Interessen des Beschwerdeführers in diesem Fall überwiegen.

Dieser Bescheid ist rechtskräftig.

14. Bescheid vom 13.5.2019, GZ: DSB-D123.688/ 0003-DSB/2018 (Kreditauskunftei als Verantwortliche für die durchgeführte Bonitätsbewertung, nicht rechtskräftig, Newsletter 3/2019, Seite 4 f)

In diesem Bescheid hatte sich die Datenschutzbehörde u.a. mit der Frage zu beschäftigen, ob eine Kreditauskunftei für die von ihr durchgeführte Bonitätsbewertung als datenschutzrechtlicher Verantwortlicher zu qualifizieren ist.

Gegenstand des genannten Verfahrens ist eine behauptete Verletzung im Recht auf Auskunft. Neben mehreren seitens des Beschwerdeführers behaupteten Verletzungen, die sich im Wesentlichen auf eine unvollständige Auskunft beschränken, wurde geltend gemacht, dass die Beschwerdegegnerin, welche eine Kreditauskunftei betreibt, keine näheren Angaben im Hinblick auf die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der durchgeführten Bonitätsbewertung des Beschwerdeführers beauskunftet habe. Die Beschwerdegegnerin hielt dem zusammengefasst entgegen, dass die Entscheidung über das Zustandekommen eines Rechtsgeschäfts bzw. in welcher Form das Rechtsgeschäft zustande kommt, ausschließlich das bei der Beschwerdegegnerin abfragende Unternehmen treffe.

Die Datenschutzbehörde hielt diesbezüglich fest, dass die Beschwerdegegnerin personenbezogene Daten zum Zweck der Ausübung ihres Gewerbes nach § 152 GewO 1994 (Auskunftei über Kreditverhältnisse) verarbeitet und dass aufgrund der statistischen Wahrscheinlichkeit anhand gewisser Parameter ein mathematischer Wert errechnet wird, der die Zahlungsausfallswahrscheinlichkeit widerspiegelt. Der Umstand, dass Unternehmen die Möglichkeit haben, die Gewichtung bzw. weitere Parameter (etwa eigene Zahlungserfahrungen mit dem Endkunden/der betroffenen Person) in die Logik einfließen zu lassen, schadet dabei nicht. Im Sinne der obigen Überlegungen kann die Beschwerdegegnerin nämlich nicht als Auftragsverarbeiter verstanden werden, da die Daten nicht bloß im Auftrag des jeweiligen Kunden verarbeitet werden, sondern eine Verarbeitung unabhängig davon im Rahmen der Ausübung des Gewerbes nach § 152 GewO 1994 durchgeführt wird und die „Score-Formel“ - das heißt welche konkreten Informationen mit Personenbezug auf welche konkrete Weise miteinander kombiniert werden, um eine bestimmte Bonität zu errechnen - von der Beschwerdegegnerin selbst festgelegt wird.

Nach Ansicht der Datenschutzbehörde handelt es sich um einen eigenständigen Entscheidungsprozess bei der Beschwerdegegnerin, da die Beschwerdegegnerin das genannte Gewerbe ausübt, um errechnete Bonitätsdaten in den wirtschaftlichen Verkehr zu bringen und dies nach der allgemeinen Lebenserfahrung mit erheblichen Beeinträchtigungen im wirtschaftlichen Leben verbunden sein kann. Sofern ein Endkunde, welcher die Bonitätsauskunft einholt, auf Basis der berechneten Bonität eine gewisse Entscheidung trifft – etwa indem er das Bonitätsergebnis unhinterfragt seiner wirtschaftlichen Entscheidung zugrunde legt – handelt es sich hierbei um einen zweiten eigenständigen Entscheidungsprozess bei dem Endkunden.

Im Ergebnis war somit der Leistungsauftrag an die Beschwerdegegnerin zu erteilen, dem Beschwerdegegner aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der den Beschwerdeführer betreffenden Bonitätsbewertung zu geben.

Dieser Bescheid ist nicht rechtskräftig.

15. Bescheid vom 20.5 2019, GZ: DSB-D123.972/0005-DSB/2019 (Mehrfache Verwendung von personenbezogenen Daten aus dem Grundbuch zwecks möglicher Akquisition von Immobilien, Verletzung der Informationspflichten, nicht rechtskräftig, Newsletter 3/2019, Seite 4)

Im Gegensatz zum weiter oben berichteten Fall hatte sich die Datenschutzbehörde hier mit der Frage zu beschäftigen, ob auch bei mehrmaliger Kontaktaufnahme durch eine Immobilien-treuhänderin deren Interessen gegenüber jenen des Betroffenen überwiegen. Konkret kontaktierte die Beschwerdegegnerin den Beschwerdeführer mittels Briefen innerhalb eines Monats zweimal und innerhalb eines Zeitraumes von etwas mehr als einem Jahr dreimal, um dessen Verkaufsabsichten zu ermitteln. Hier fiel die Interessenabwägung zugunsten des Betroffenen aus, welcher ein berechtigtes Interesse daran hat, dass seine personenbezogenen Daten nicht dauerhaft zum Zwecke regelmäßiger Anfragen betreffend eines allfälligen Grundstücksverkaufs verarbeitet werden. Dieses Interesse überwiegt in der vorliegenden Konstellation gegenüber dem wirtschaftlichen Interesse der Beschwerdegegnerin, wodurch der Beschwerdeführer in seinem Recht auf Geheimhaltung verletzt wurde.

Weiters wurde der Beschwerdegegnerin im selben Bescheid aufgetragen, dem Beschwerdeführer Informationen über die Rechtsgrundlage der erfolgten Verarbeitung seiner personenbezogenen Daten (Art. 14 Abs. 1 lit. c DSGVO), über die Dauer, für die die personenbezogenen Daten gespeichert werden, oder falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (Art. 14 Abs. 2 lit. b DSGVO) und, sollte die Verarbeitung der personenbezogenen Daten des Beschwerdeführers auf Art. 6 Abs. 1 lit. f DSGVO beruhen, die berechtigten Interessen, die von der Beschwerdegegnerin bei der Verarbeitung verfolgt wurden (Art. 14 Abs. 2 lit. b DSGVO) zu erteilen, da der Beschwerdeführer über diese Informationen weder in den drei Schreiben an ihn noch während des Verfahrens vor der Datenschutzbehörde informiert wurde und der Beschwerdeführer eine Verletzung der Informationspflichten durch die Beschwerdegegnerin geltend gemacht hat.

Dieser Bescheid ist nicht rechtskräftig.

16. Bescheid vom 27.6.2019, GZ: DSB-D124.071/0005-DSB/2019 (Löschung statt Auskunft als Verletzung im Auskunftsrecht, rechtskräftig, RIS)

In diesem Bescheid hatte sich die Datenschutzbehörde (erstmalig seit Außerkrafttreten von § 26 Abs. 7 DSG 2000) mit der Frage zu befassen, ob ein Verantwortlicher als Reaktion auf einen Antrag auf Auskunft die zur Person des Auskunftswerbers verarbeiteten Daten löschen darf.

Der Beschwerdeführer hatte von einer Versicherungsmaklergesellschaft (Beschwerdegegnerin) eine datenschutzrechtliche Auskunft verlangt und eine Negativauskunft erhalten. Diese hielt er für unzutreffend und erhob Beschwerde. Das Ermittlungsverfahren ergab, dass die Beschwerdegegnerin nach Einlangen des Antrags auf Auskunft sämtliche Daten des Beschwerdeführers gelöscht hatte.

Die Datenschutzbehörde hielt in der Bescheidbegründung fest, dass die DSGVO zwar, anders als die alte Rechtslage, kein ausdrückliches Lösungsverbot ab Einlangen eines Auskunftsverlangens enthält, eine Löschung wie im Beschwerdefall aber gegen die Grundsätze der Datenverarbeitung nach Treu und Glauben, insbesondere gegen die Transparenzpflicht nach Art. 5 Abs. 1 lit. a DSGVO, verstößt.

Der Beschwerde wurde daher Folge gegeben und eine Verletzung des Auskunftsrechts festgestellt.

Dieser Bescheid ist rechtskräftig.

17. Bescheid vom 4.7.2019, GZ: DSB-D123.652/0001-DSB/2019 (Zulässigkeit der automatisierten Kennzeichenerfassung bei einer Parkgarage, rechtskräftig, Newsletter 4/2019, Seite 5 f, RIS)

In diesem Bescheid hatte sich die Datenschutzbehörde mit der Frage der Zulässigkeit einer automatisierten Kennzeichenerfassung bei einer Parkgarage zwecks Abrechnung der Garagennutzung zu befassen.

Bei der Beschwerdegegnerin handelt es sich um die Betreiberin eines größeren Einkaufszentrums, welche die Nutzung einer Parkgarage zur Verfügung stellt. Bei der Einfahrt in die Parkgarage der Beschwerdegegnerin wurde vor Passieren des Einfahrtsschranks durch eine Kamera automatisiert das Kennzeichen des PKW des Beschwerdeführers erfasst. Der Beschwerdeführer behauptete eine Verletzung im Recht auf Geheimhaltung sowie einen Verstoß gegen das Koppelungsverbot, da – zusammengefasst - die Benutzung der Parkgarage nur dann möglich sei, wenn man die automatisierte Erfassung des Kennzeichens dulde. Die Beschwerdegegnerin stützte die gegenständliche Verarbeitung auf berechnete Interessen nach Art. 6 Abs. 1 lit. f DSGVO.

Die Datenschutzbehörde hielt zunächst fest, dass neben dem Kennzeichen weitere personenbezogene Daten verarbeitet werden, nämlich der genaue Zeitpunkt und Ort, an dem sich der Beschwerdeführer als Halter (und gegenständlich auch Fahrer) befunden habe. Ebenso wurden die Informations- und Kennzeichnungspflichten offenbar nicht ordnungsgemäß umgesetzt, da der Verarbeitungszweck, nämlich die Erfassung des Kennzeichens zwecks Abrechnung der Garagennutzung, nicht am Schild vor der Einfahrt angeführt wurde.

Dies ist nach Ansicht der Datenschutzbehörde jedoch belanglos: Zwar ist im Rahmen einer Interessenabwägung auch auf die vernünftige Erwartungshaltung abzustellen, allerdings ist die automatisierte Kennzeichenerfassung zwecks Abrechnung der Garagennutzung nicht unüblich (vgl. den Bescheid der DSB vom 18. März 2019, GZ: DSB-D196.007/0005-DSB/2019, mit welchem Verhaltensregeln gemäß Art. 40 Abs. 5 DSGVO betreffend Garagen- und Parkplatzbetriebe in Österreich inhaltlich genehmigt wurden). Darüber hinaus hat die Beschwerdegegnerin auch geeignete technische und organisatorische Maßnahmen angeführt, um die Interessen des Beschwerdeführers entsprechend zu wahren (u.a. sofortige Löschung der personenbezogenen Daten nach Abwicklung der Abrechnung).

Die Datenschutzbehörde sieht die berechtigten Interessen in der Raschheit und Effizienz einer solchen Verarbeitung gelegen, um solche Kurznutzungsverträge (Parkgaragenbenutzung) abzuwickeln. Umgekehrt hat der Beschwerdeführer keine berechtigten Interessen ins Treffen geführt, insbesondere hat die Beschwerdegegnerin die Daten des Beschwerdeführers auch zu keinem anderen Zweck als zur Abwicklung der Abrechnung verarbeitet.

Auf einen etwaigen Verstoß gegen das in Art. 7 Abs. 4 DSGVO normierte „Koppelungsverbot“ war nicht einzugehen, da die Beschwerdegegnerin die Verarbeitung nicht auf eine Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO gestützt hat. Eine Verletzung der Informationspflichten nach Art. 13 DSGVO war nicht Gegenstand des Verfahrens.

Die Beschwerde wurde daher abgewiesen und die Entscheidung ist rechtskräftig.

Siehe auch Abschnitt 3.2.9., Genehmigung der datenschutzrechtlichen Verhaltensregeln für Garagenbetreiber, wo ebenfalls eine automatisierte Kennzeichenerfassung vorgesehen ist.

18. Bescheid vom 23.7.2019, GZ: DSB-D123.822/0005-DSB/2019 (Kein Recht auf partielle Löschung bestimmter Daten im Rahmen eines Kunden-Bonusprogramms, rechtskräftig, Newsletter 4/2019, Seite 5, RIS)

In diesem Bescheid hatte sich die Datenschutzbehörde mit der Frage zu beschäftigen, ob ein Recht darauf besteht, dass bestimmte Daten im Rahmen eines Kunden-Bonusprogramms gelöscht werden.

Bei der Beschwerdegegnerin handelt es sich um ein Einzelhandelsunternehmen, welches ein Kunden-Bonusprogramm betreibt. Der Beschwerdeführer nahm an diesem Kunden-Bonusprogramm teil und begehrte in weiterer Folge die Löschung gewisser personenbezogener Daten (u.a. im Hinblick auf Einkaufsort- und Zeitpunkt), während andere personenbezogene Daten (u.a. Stammdaten) im System der Beschwerdegegnerin weiterhin verarbeitet werden sollten. Die Beschwerdegegnerin führte - zusammengefasst - ins Treffen, dass es aufgrund des Aufbaus der Datenbank nicht möglich sei, partiell personenbezogene Daten zu löschen.

Die Datenschutzbehörde hielt zunächst fest, dass ein partieller Antrag auf Löschung im Hinblick auf gewisse Daten grundsätzlich möglich ist und sich ein Verantwortlicher seiner in der DSGVO postulierten Verpflichtungen nicht dadurch entziehen kann, indem er keine entsprechenden technischen und organisatorischen Vorkehrungen trifft, um den Anträgen nach Art. 12 Abs. 3 DSGVO entsprechen zu können.

Gleichzeitig wurde festgehalten, dass die Folge einer vollständigen Löschung, welche die Beschwerdegegnerin angeboten hat, jedoch keine Erschwernis oder Verhinderung des wirtschaftlichen Fortkommens darstellt. Anders formuliert: Konsequenz einer vollständigen Löschung ist lediglich, dass eine Teilnahme am Kunden-Bonusprogramm nicht mehr möglich ist, eine solche Nichtteilnahme nach derzeitiger allgemeiner Lebenserfahrung aber nicht mit nennenswerten wirtschaftlichen Nachteilen verbunden ist.

Anders zu beurteilen ist etwa die vollständige Löschung aus einer Bonitätsdatenbank, da mangels Treffers zu einer Abfrage dies zu einem Nichtabschluss eines Vertrags führen kann (vgl. den Bescheid vom 5. Dezember 2018 zur GZ: DSB-D123.211/0004-DSB/2018, nicht rechtskräftig).

Im Ergebnis gestand die Datenschutzbehörde der Beschwerdegegnerin einen Spielraum für die Ausgestaltung ihres Kunden-Bonusprogramms im Rahmen der Privatautonomie und im Rahmen ihrer Erwerbsfreiheit zu und war diese nicht angehalten, entsprechende technische und organisatorische Maßnahmen zu treffen, d.h. ihr System umzugestalten, um eine partielle Löschung zu ermöglichen.

Die Beschwerde wurde daher abgewiesen, und die Entscheidung ist rechtskräftig.

19. Bescheid vom 31.7.2019, GZ: DSB-D123.901/0002-DSB/2019(Auskunft, „begründete Zweifel“ betreffend Identität, kein Auskunftsinteresse nachzuweisen, rechtskräftig, RIS)

Eine Bausparkasse hatte eine datenschutzrechtliche Auskunftserteilung mit der Begründung abgewiesen, der Auskunftswerber (Beschwerdeführer) habe nicht, wie von ihr verlangt, ein eigenhändig unterschriebenes Schreiben samt Ausweiskopie übermittelt. Der Beschwerdeführer, ein Rechtsanwalt, verwies u.a. auf den PGP-Schlüssel (keine qualifizierte elektronische Signatur), der der E-Mail mit seinem Auskunftsantrag angeschlossen war. Die Datenschutzbehörde hielt dazu fest, ein PGP-Schlüssel diene in diesem Zusammenhang einerseits der Vertraulichkeit

durch Verschlüsselung, andererseits der Authentifizierung mittels Signierung. Die Bausparkasse habe also davon ausgehen können, dass die E-Mail tatsächlich von der Adresse „p.a***@a**-h**-o**.at“ versandt wurde. Der Beschwerdeführer sei nachweislich und jederzeit überprüfbar Partner in der Anwaltsgesellschaft, der diese Domain zuzurechnen sei. Die DSGVO gebe keine konkrete Form der Identifizierung vor und erlaube dem Verantwortlichen gemäß Art. 12 Abs. 6 nur bei „begründeten Zweifeln“ die Anforderung eines (zusätzlichen) Identitätsnachweises. Bei obiger Form der Identifizierung konnte sich die Bausparkasse nicht mehr auf begründete Zweifel berufen.

Auch das weitere Argument der Bausparkasse, der Beschwerdeführer habe kein Rechtsschutzinteresse, da es ihm nur darum gehe, über das Verfahren in seinem Blog zu berichten, wurde für nicht stichhaltig befunden. Das Auskunftsrecht gemäß Art. 15 DSGVO ist an kein Auskunfts- oder Rechtsschutzinteresse als Voraussetzung gebunden.

Es wurde daher eine Verletzung im Auskunftsrecht festgestellt und die Auskunftserteilung aufgetragen.

Dieser Bescheid ist rechtskräftig.

20. Bescheid vom 2.8.2019, GZ: DSB-D123.594/0003-DSB/2019 (Offenlegung der Zusammensetzung einer Schulnote, nicht rechtskräftig, Newsletter 4/2019, Seite 4 f)

Im dieser Sache hatte die Datenschutzbehörde im Zuge eines Beschwerdeverfahrens die Frage zu klären, ob die Beschwerdeführerin dadurch in ihrem Recht auf Geheimhaltung verletzt wurde, indem der Beschwerdegegner, ihr Lehrer, die genaue Zusammensetzung einer ihrer Schulnoten den Klassensprechern mündlich mitgeteilt hatte, um Unstimmigkeiten in der Klasse zu beseitigen. Der Inhalt dieses Gesprächs wurde dann von den Klassensprechern in einer Gruppe in einem sozialen Netzwerk geteilt.

Die Datenschutzbehörde hielt zunächst fest, dass ein Eingriff in das Grundrecht auf Geheimhaltung von Daten in nahezu jeder Form, somit auch durch mündliche Übermittlung erfolgen kann. Weiters stellte sie fest, dass es sich auch bei einer Schulnote um ein personenbezogenes Datum gemäß Art. 4 Abs. 1 DSGVO handelt.

Die Datenschutzbehörde verneinte eine allgemeine Verfügbarkeit der den Klassensprechern mitgeteilten Daten. Gesprächsgegenstand zwischen Beschwerdegegner und Klassensprechern war nicht nur die Schulnote der Beschwerdeführerin per se, sondern vielmehr eine detaillierte Information über das Zustandekommen dieser Note. Eine derartige Vorgangsweise ist von § 6 Abs. 2 der Leistungsbeurteilungsverordnung, auf welche sich der Beschwerdegegner berief, nicht gedeckt. Dem Vorbringen des Beschwerdegegners, er habe keine wesentlichen neuen Informationen weitergegeben, konnte nicht gefolgt werden. Die Datenschutzbehörde ging davon aus, dass den Klassensprechern die genaue Notenzusammensetzung sicherlich nicht bekannt gewesen ist, und die Mitteilung sehr wohl neue Informationen enthielt. Die Schutzwürdigkeit der Daten war somit jedenfalls zu bejahen.

Die Datenschutzbehörde übersah nicht, dass die Mitteilung an die Klassensprecher von der nachvollziehbaren Intention getragen war, Unstimmigkeiten im Klassenverband zu bereinigen, jedoch wäre als gelinderes Mittel eine Information der betroffenen Schülerin über die genaue Zusammensetzung der Note in Betracht gekommen.

Vor diesem Hintergrund gelangte die Datenschutzbehörde zu dem Ergebnis, dass eine Verletzung im Recht auf Geheimhaltung vorlag.

Dieser Bescheid ist nicht rechtskräftig.

21. Bescheid vom 7.8.2019, GZ: DSB-D123.737/0003-DSB/2019 (Ladung zur Bauverhandlung, Wohnadressen, elektronische Kundmachung, Suchmaschinenergebnisse, rechtskräftig, RIS)

In dieser Sache führte ein Ehepaar Beschwerde wegen Verletzung des Geheimhaltungsrechts (Rechtmäßigkeit der Datenverarbeitung), weil die Baubehörde einer steirischen Gemeinde in der Ladung zu einer Bauverhandlung ihre Wohnadressen angeführt und diese Ladung auch im elektronischen Amtsblatt kundgemacht hatte. Anlass war, dass diese Daten auch von der Google-Suchmaschine gefunden werden konnten.

Die Datenschutzbehörde gab der Beschwerde im Hauptpunkt Folge. Es bestehe in den einschlägigen Verwaltungsgesetzen (§§ 25 und 27 Stmk. BauG) zwar eine Verpflichtung, die Ladung zur Bauverhandlung öffentlich kundzumachen, was auch elektronisch geschehen könne, und darin die bekannten Nachbarn anzuführen. Für eine Bekanntmachung der Adressen bestehe aber keine ausdrückliche Grundlage und auch keine erkennbare Notwendigkeit.

Hinsichtlich der von den Beschwerdeführern behaupteten Verantwortung der Gemeinde für die Erfassung der Daten durch Internet-Suchmaschinen wurde die Beschwerde jedoch abgewiesen. Der EuGH habe bereits im Urteil vom 13.5.2014, C-131/12, festgehalten, dass ein Suchmaschinenbetreiber als eigenständiger datenschutzrechtlich Verantwortlicher zu qualifizieren ist.

Dieser Bescheid ist rechtskräftig.

22. Bescheid vom 19.8.2019, GZ: DSB-D123.957/0003-DSB/2019 (Verarbeitung personenbezogener Daten aus der PsychotherapeutInnenliste für privates Online-PsychotherapeutInnen-Verzeichnis, nicht rechtskräftig, Newsletter 4/2019, Seite 3)

In diesem Bescheid hatte sich die Datenschutzbehörde mit einer behaupteten Verletzung im Recht auf Geheimhaltung (§ 1 DSG) und im Recht auf Information (Art. 14 DSGVO) zu befassen.

Der Beschwerdeführer ist als praktizierender Psychotherapeut in der vom Bundesministerium für Arbeit, Soziales und Konsumentenschutz (BMASGK, seit 29.1.2010: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz) unter der Webadresse „psychotherapie.ehealth.gv.at“ veröffentlichten Liste eingetragen. Die Beschwerdegegnerin ist Betreiberin eines Service- und Infoportals betreffend Psychotherapie, worin ein für Besucher dieser Website kostenloses und im Verhältnis zur Liste des BMASGK technisch moderneres Online-PsychotherapeutInnen-Verzeichnis eingebettet ist.

Der Beschwerdeführer erachtete sich deswegen in seinem Recht auf Geheimhaltung (§ 1 DSG) verletzt, weil die Beschwerdegegnerin für das Grundgerüst ihres Online-Verzeichnisses unter anderem die (personenbezogenen) Daten des Beschwerdeführers – insbesondere ohne dessen Einwilligung – aus der Liste des BMASGK übernommen hatte. Darüber hinaus behauptete der Beschwerdeführer, dass die Beschwerdegegnerin insgesamt keine (hinreichende) Information gem. Art. 14 DSGVO erteilt habe.

Die Datenschutzbehörde wies die Beschwerde hinsichtlich der behaupteten Verletzung im Recht auf Geheimhaltung ab, weil die umfangreiche Interessenabwägung zugunsten der Beschwerdegegnerin ausgegangen war. Hinsichtlich der behaupteten Verletzung im Recht auf Information gem. Art. 14 DSGVO gab die Datenschutzbehörde der Beschwerde teilweise statt, da auch die im Verfahren nachträglich vorgelegte Datenschutzerklärung nicht in allen Punkten hinreichend war.

Dieser Bescheid ist nicht rechtskräftig.

23. Bescheid vom 27.8.2019, GZ: DSB-D123.942/0004-DSB/2019 (Rechtmäßigkeit der Verarbeitung, Rehabilitationszentrum, elektronische Anwesenheitskontrolle, rechtskräftig, RIS)

Der Beschwerdeführer war Patient im Rehabilitationszentrum eines Sozialversicherungsträgers (Beschwerdegegner). Alle Zimmer dort sind mit Bewegungsmeldern und elektronischen Türschlössern, welche mittels codiertem Chip-Schlüssel versperrbar sind, ausgestattet. Es werden keine Bewegungsprofile erstellt und keine Aufzeichnungen über Bewegungsmuster erhoben. Zweck der Anlage ist eine elektronische Zimmerbelegungserkennung. Von berechtigten Mitarbeitern des Beschwerdegegners kann diese Information im Anlassfall abgerufen werden. Der Beschwerdeführer sah dadurch sein Geheimhaltungsrecht verletzt und erhob Beschwerde.

Die Datenschutzbehörde hielt fest, dass die Datenverarbeitung zwar nicht geeignet ist, lebenswichtige Interessen der Patienten zu schützen, die Patienten jedoch gemäß Sozialversicherungsrecht durch den Therapieplan in ihrer Bewegungsfreiheit beschränkt und zur Mitwirkung am Therapieerfolg verpflichtet sind, wozu auch die Einhaltung der vorgeschriebenen Nachtruhe gehört, deren Kontrolle durch die Datenverarbeitung ermöglicht wird. Die Datenschutzbehörde gelangte daher zum Schluss, dass die verfahrensgegenständliche Datenverarbeitung geeignet und verhältnismäßig ist, um die wechselseitigen Rechte und Pflichten der involvierten Parteien im Rahmen einer Rehabilitation zu wahren. Die Beschwerde wurde daher abgewiesen.

Dieser Bescheid ist rechtskräftig.

24. Bescheid vom 29.8.2019, GZ: DSB-D123.874/0016-DSB/2019 (Recht auf Auskunft betreffend Dokumente, die von einer Religionsgemeinschaft in einem verschlossenen Umschlag aufbewahrt werden, nicht rechtskräftig, Newsletter 4/2019, Seite 3 f)

Mit diesem Bescheid hatte die Datenschutzbehörde unter anderem zu entscheiden, ob der Beschwerdeführer dadurch in seinem Recht auf Auskunft verletzt wurde, indem ihm die Beschwerdegegnerin, eine in Österreich anerkannte Religionsgemeinschaft, gewisse Unterlagen, welche sie in einem verschlossenen Umschlag aufbewahrt, nicht als Kopien bereitgestellt hat. Der Beschwerdeführer war aus der Religionsgemeinschaft der Beschwerdegegnerin ausgetreten.

Zunächst setzte sich die Datenschutzbehörde mit der Frage auseinander, ob die auf der Webseite der Verantwortlichen veröffentlichten weltweiten Datenschutzrichtlinien als Regelungen iSd Art. 91 Abs. 1 DSGVO zu qualifizieren sind und verneinte dies mit der Begründung, dass diese als nicht umfassend genug erscheinen, weshalb der Fall anhand der DSGVO zu beurteilen war.

Sodann war zu prüfen, ob der verschlossene Umschlag ein Dateisystem iSd Art. 4 Z 6 DSGVO ist. Unter Dateisystem ist nach der Begriffsbestimmung des Art. 4 Z 6 DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird, zu verstehen. Der EuGH beschäftigte sich in seinem Urteil vom 10.6.2018 (C-25/17) mit dem Begriff des Dateisystems und führte darin aus, dass eine Datei dann nach bestimmten Kriterien sortiert ist, wenn sie leicht wiederauffindbar ist. Die personenbezogenen Daten müssen nicht in spezifischen Kartotheken oder Verzeichnissen oder einem anderen Rechtersystem enthalten sein. An diesem Kriterium orientierte sich die Datenschutzbehörde. Der verfahrensgegenständliche Umschlag ist mit Namen des Beschwerdeführers, dem Grund des Ausscheidens aus der Gemeinschaft und dem Austrittsdatum beschriftet. Dies dient der leichteren Wiederauffindbarkeit und der gezielten Suche von Personen. Es ist davon auszugehen, dass etliche Umschläge dieser Art von der Beschwerdegegnerin aufbewahrt werden, weshalb die Datenschutzbehörde zum Schluss kam, dass betreffend den verschlossenen Umschlag der sachliche Anwendungsbereich gemäß Art. 2 Abs. 1 DSGVO eröffnet ist.

Die Beschwerdegegnerin brachte vor, sie stelle dem Beschwerdeführer deshalb keine Kopien der Unterlagen im verschlossenen Umschlag bereit, weil ihr Vorgehen religionsrechtlichem Gewohnheitsrecht entspreche und weltweit seit Jahrzehnten geübte Praxis der Religionsgemeinschaft sei, häufig Sachverhalte vorliegen würden, die der Privat- bzw. Intimsphäre der Beteiligten zuzurechnen seien und der Schutz des Seelsorgergeheimnisses von höchster Bedeutung sei.

Nach Art. 15 Abs. 4 DSGVO darf das Recht auf Erhalt einer Kopie gemäß Abs. 3 die Rechte und Freiheiten einer anderen Person nicht beeinträchtigen. Dies schließt auch die Rechte des Verantwortlichen ein. ErwGr. 63 legt bei solchen Spannungsverhältnissen eine Interessenabwägung nahe und nennt beispielsweise Geschäftsgeheimnisse sowie Rechte des geistigen Eigentums. Die Datenschutzbehörde hatte zu prüfen, ob Rechte und Freiheiten der Beschwerdegegnerin im Sinne des Art. 15 Abs. 4 DSGVO einer Bereitstellung von Datenkopien entgegenstehen. Nach ErwGr. 4 steht die DSGVO im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt werden, darunter unter anderem auch die Gewissens- und Religionsfreiheit.

Als Rechte der Beschwerdegegnerin kommen im vorliegenden Fall die ihr aus den Art. 15 StGG, Art. 9 EMRK und Art. 17 AEUV erwachsenden in Betracht. Diese schützen nicht nur die Rechte von einzelnen Gläubigen und Nichtgläubigen, sondern begründen auch ein Grundrecht auf korporative Religionsfreiheit.

Es stellte sich die Frage, ob durch eine Stattgabe der Beschwerde in die inneren Angelegenheiten der Religionsgemeinschaft eingegriffen würde. Die Datenschutzbehörde kam im gegenständlichen Fall zum Schluss, dass die Praxis der Beschwerdegegnerin, Umschläge, die Dokumente betreffend das Ausscheiden eines Mitgliedes aus ihrer Gemeinschaft enthalten, verschlossen aufzubewahren, eine innere Angelegenheit darstellt. Insofern handelt es sich um eine Frage, die die Datenschutzbehörde als staatliche Behörde nicht beurteilen darf. Eine Kopie der im verschlossenen Umschlag enthaltenen personenbezogenen Daten des Beschwerdeführers war daher nicht bereitzustellen und die Beschwerde war abzuweisen.

Dieser Bescheid ist nicht rechtskräftig.

25. Bescheid vom 2.9.2019, GZ: DSB-D123.862/0008-DSB/2019 (Zustellung der begehrtten Auskunft während des Verfahrens durch die Datenschutzbehörde, rechtskräftig, Newsletter 4/2019, Seite 3)

In dieser Sache hatte sich die Datenschutzbehörde mit der Frage zu beschäftigen, ob der Beschwerdeführer dadurch im Recht auf Auskunft verletzt wurde, indem ihm die Auskunft während des Verfahrens vor der Datenschutzbehörde nicht durch die Beschwerdegegnerin selbst, sondern durch die Datenschutzbehörde zugestellt wurde.

Konkret wurde die während des Verfahrens vor der Datenschutzbehörde durch die Beschwerdegegnerin versendete postalische Briefsendung mit der Auskunft vom Beschwerdeführer nicht behoben.

Die Beschwerdegegnerin übermittelte diese Sendung auch der Datenschutzbehörde. Im Rahmen des sodann dem Beschwerdeführer gewährten Parteiengehörs nach § 24 Abs. 6 DSG wurde dem Beschwerdeführer die verfahrensgegenständliche Auskunft durch die Datenschutzbehörde zugestellt. Den Inhalt der Auskunft bemängelte der Beschwerdeführer nicht, jedoch bemängelte er, dass ihm diese nie durch die Beschwerdegegnerin zugestellt worden war.

Der österreichische Gesetzgeber hat für den Verantwortlichen in § 24 Abs. 6 DSG die Möglichkeit geschaffen, die behauptete Rechtsverletzung bis zum Abschluss des Verfahrens vor der Datenschutzbehörde zu beseitigen, indem er den Anträgen des Beschwerdeführers entspricht. Dem Wortlaut des § 24 Abs. 6 DSG ist nicht zu entnehmen, dass diese Reaktion während des Verfahrens vor der Datenschutzbehörde zwingend gegenüber dem Beschwerdeführer zu erfolgen hat. Auch durch eine

Übermittlung dieser Reaktion an die Datenschutzbehörde, welche das Schreiben im Rahmen des Parteihörs sodann an den Beschwerdeführer weiterleitet, kann eine behauptete Rechtsverletzung nachträglich beseitigt werden. Zweck des § 24 Abs. 6 DSG ist, dass der Beschwerdeführer Gelegenheit erhält, zur Reaktion des Beschwerdegegners Stellung zu nehmen und Gründe anzuführen, warum er die ursprünglich behauptete Rechtsverletzung nach wie vor als nicht beseitigt erachtet. Dieser Zweck wird nicht dadurch vereitelt, indem ihm die Reaktion auf seinen Antrag durch die Datenschutzbehörde übermittelt wird und nicht durch den Beschwerdegegner selbst. Das Rechtsschutzinteresse des Beschwerdeführers bleibt gewahrt. Die Datenschutzbehörde sprach im konkreten Fall aus, dass der Beschwerdeführer nicht in seinem Recht auf Auskunft verletzt wurde und wies die Beschwerde ab.

Dieser Bescheid ist rechtskräftig.

26. Bescheid vom 4.9.2019, GZ: DSB-D124.1183/0002-DSB/2019 (Widerspruch, Verarbeitung des Geburtsdatums eines Minderjährigen, keine Bevollmächtigung eines Vertretungsbedürftigen durch den gesetzlichen Vertreter, rechtskräftig, RIS)

Der minderjährige Beschwerdeführer hat seit 2018 eine Reihe von Beschwerden bei der Datenschutzbehörde anhängig gemacht. Nachdem hinsichtlich des Alters des Beschwerdeführers Bedenken entstanden waren, ermittelte die Datenschutzbehörde dieses von Amts wegen und verlangt seither die Mitwirkung eines Obsorgeberechtigten bei allen Verfahrenshandlungen.

Der Beschwerdeführer legte nun gegen die Verarbeitung seines Geburtsdatums mit dem Argument, es sei evident, dass die Datenschutzbehörde dieses „nur zu seinem Nachteil“ verarbeite, Widerspruch ein. Die Datenschutzbehörde lehnte diesen mit Begründung ab. Darauf brachte der Beschwerdeführer, wiederum unvertreten, eine Beschwerde gegen die Datenschutzbehörde wegen Verletzung des Widerspruchsrechts gemäß Art. 21 DSGVO bei der Datenschutzbehörde ein.

Auf Mangelbehebungsauftrag der Datenschutzbehörde, die Zustimmung eines Obsorgeberechtigten zur Beschwerdeführung nachzuweisen, legte der Beschwerdeführer eine von seinem obsorgeberechtigten Vater ausgestellte Urkunde vor, seinem Sohn Vollmacht zu erteilen, „sich selbst im Rahmen der Beschwerdeführung gemäß Art. 77 DSGVO und § 24 DSG vor der Datenschutzbehörde in meinem Namen zu vertreten.“

Die Datenschutzbehörde hat die Beschwerde daraufhin wegen eines nicht behobenen Mangels zurückgewiesen. Im Ergebnis sei die vorliegende Vollmachtserklärung als unzulässige „Pauschalermächtigung“ zu qualifizieren.

Dieser Bescheid ist rechtskräftig.

27. Bescheid vom 1.10.2019, GZ: DSB-D124.567/0005-DSB/2019 (Auftrag zur Löschung eines Warnlisteneintrags an eine Bank, rechtskräftig, RIS)

In diesem Bescheid hatte sich die Datenschutzbehörde mit einer Beschwerde gegen die verweigerte Löschung eines Eintrags in der „Warnliste“ der Banken (gemeinsame Verarbeitung der Banken zur Risikominimierung, in diese werden etwa Kunden eingetragen, die Kredite nicht oder nicht vollständig zurückzahlen konnten, man spricht diesbezüglich auch von „Zahlungserfahrungsdaten“). Die zu löschende Eintragung stammte aus dem Jahr 2000. Zum Nachweis ihrer Richtigkeit konnte die Bank nur eine alte Karteikarte betreffend ein im Jahr 1987 (!) bei einem Schuldenstand von umgerechnet € 5087,01 geschlossenes Kreditkonto vorlegen. Die Datenschutzbehörde führte eine Interessenabwägung durch und hielt fest: „Bei 35 Jahre alten Zahlungserfahrungsdaten kann jedenfalls keine Rede davon sein, dass diese geeignet wären, ein aktuelles Bild von Realität abzugeben.“ Da damit das Löschungsinteresse des Beschwer-

deführers überwog, wurde eine Verletzung des Löschungsrechts festgestellt und der Bank die Löschung des Warnlisteneintrags aufgetragen.

Dieser Bescheid ist rechtskräftig.

28. Bescheid vom 3.10.2019, GZ: DSB-D123.795/0002-DSB/2019 (Berichtigung, kein Recht auf bestimmte Schreibweise eines Familiennamens, nicht rechtskräftig)

In diesem Bescheid hatte sich die Datenschutzbehörde mit Frage zu befassen, ob das Recht auf Berichtigung gemäß Art. 16 DSGVO auch das Recht umfasst, eine bestimmte Schreibweise eines Familiennamens durchzusetzen.

Der Beschwerdeführer war bei einem Großkonzern beschäftigt, die Beschwerdegegnerin ist die für Verarbeitung von Personaldaten verantwortliche Konzerngesellschaft. Der Familienname des Beschwerdeführers wird mit einem „ß“ geschrieben, in den Verarbeitungen der Beschwerdegegnerin wurde dieses durch ein Doppel-S ersetzt. Die Beschwerdegegnerin lehnte einen Berichtigungsantrag ab und rechtfertigte dies auch vor der Datenschutzbehörde damit, dass die zur Datenverarbeitung eingesetzte, in der Personalverwaltung weit verbreitete Software ein „ß“ nicht vorsehe, da nicht zwischen Groß- und Kleinschreibung unterschieden werde. Die Verwendung von Buchstabenkombinationen an Stelle von Sonderzeichen sei weit verbreitet, etwa im maschinenlesbaren Teil amtlicher Lichtbildausweise. Der Beschwerdeführer hielt dem u.a. entgegen, dass sein Name in solchen Ausweisen stets mit „ß“ geschrieben werde, sein Name werde daher von der Beschwerdegegnerin unrichtig verarbeitet.

Die Datenschutzbehörde hielt in ihren rechtlichen Erwägungen fest, dass eine abweichende aber (etwa an Hand der von der internationalen Zivilluftfahrtorganisation ICAO definierten Kriterien zur Ersetzung von Sonderzeichen, deren Anwendung auch die österr. Passverordnung anordnet) begründbare Schreibweise eines Namens keine objektive Unrichtigkeit der verarbeiteten Daten zur Folge hat. Die verwendeten Zeichenfolgen seien bedeutungsgleich. Die Beschwerde wurde daher abgewiesen.

Dieser Bescheid ist nicht rechtskräftig.

29. Bescheid vom 7.10.2019, GZ: DSB-D124.285/0005-DSB/2019 (Unzulässige Offenlegung von Gesundheitsdaten in einer WhatsApp-Chatgruppe, nicht rechtskräftig, Newsletter 1/2020, Seite 4)

In diesem Bescheid hatte sich die Datenschutzbehörde mit der Frage zu beschäftigen, ob eine Arbeitsunfähigkeitsmeldung (ohne Diagnose) als Gesundheitsdatum im Sinne von Art. 9 Abs. 1 DSGVO zu qualifizieren ist und ob die Offenlegung einer solchen Arbeitsunfähigkeitsmeldung in einer WhatsApp-Chatgruppe zu Unrecht erfolgt ist.

Bei der Beschwerdegegnerin handelt es sich um die ehemalige Arbeitgeberin des Beschwerdeführers. Dieser meldete sich krank und übermittelte die Arbeitsunfähigkeitsmeldung an seinen Vorgesetzten bei der Beschwerdegegnerin. Dieser Vorgesetzte, der der Beschwerdegegnerin zuzurechnen ist, teilte die genannte Arbeitsunfähigkeitsmeldung unter Verwendung des Kurznachrichtendienstes WhatsApp in einer WhatsApp-Chatgruppe, an welcher neben dem Beschwerdeführer auch weitere ArbeitnehmerInnen der Beschwerdegegnerin teilgenommen haben.

Die Datenschutzbehörde wies zunächst auf die Judikatur des EuGH in der Rechtssache C-101/01 (Lindqvist) hin, wonach der Begriff „Daten über Gesundheit“ weit auszulegen sei und hielt fest, dass diese Judikatur auch auf die neue Rechtslage übertragbar ist. Zwar befand sich auf

der gegenständlichen Arbeitsunfähigkeitsmeldung kein konkreter Grund für die Arbeitsunfähigkeit, allerdings besitzt nach Auffassung der Datenschutzbehörde die Information über den konkreten Zeitraum einer Arbeitsunfähigkeit (Beginn der Arbeitsunfähigkeit und Termin für die Wiederbestellung beim behandelnden Arzt) eine ausreichende Aussagekraft über den körperlichen oder geistigen Gesundheitszustand einer Person, um als „Gesundheitsdatum“ nach nunmehr Art. 4 Z 15 DSGVO qualifiziert zu werden.

Eine Rechtsgrundlage für die Offenlegung der Arbeitsunfähigkeitsmeldung, auf der neben den Gesundheitsdaten auch weitere Informationen wie die Sozialversicherungsnummer und die vollständige Anschrift des Beschwerdeführers enthalten waren, war nicht ersichtlich. Vor diesem Hintergrund war mangels Rechtsgrundlage eine Verletzung im Recht auf Geheimhaltung aufgrund einer unzulässigen Offenlegung von Gesundheitsdaten in einer WhatsApp-Chatgruppe festzustellen.

Neben diesem Verfahren wurden auch zwei weitere, parallel geführte Beschwerden gegen die Beschwerdegegnerin aufgrund desselben Sachverhalts eingebracht. Die Datenschutzbehörde machte daher zusätzlich amtswegig von ihrer Befugnis nach Art. 58 Abs. 2 lit. f DSGVO Gebrauch und hat gegen die Beschwerdegegnerin ein Verbot mit der Maßgabe verhängt, die Offenlegung von Daten ihrer ArbeitnehmerInnen im Zusammenhang mit einer Arbeitsunfähigkeitsmeldung unter Verwendung des Kurznachrichtendienstes WhatsApp zu unterlassen.

Dieser Bescheid sowie das ausgesprochene Verbot gegen die Beschwerdegegnerin sind nicht rechtskräftig.

30. Bescheid vom 9.10.2019, GZ: DSB-D130.073/0008-DSB/2019 (Fehlendes Double-Opt-In-Verfahren bei Onlinedating-Portalen, rechtskräftig, Newsletter 1/2020, Seite 3 f, RIS)

Im vorliegenden Fall ging es um ein österreichisches Unternehmen, das Onlinedating-Portale betreibt. Der minderjährige Beschwerdeführer, der seinen Wohnsitz in Deutschland hat, erhielt Sex-Spams von diesem Unternehmen, obwohl er sich nicht bei dessen Onlinedating-Portalen angemeldet hatte. Die DSB entschied für den Beschwerdeführer und sprach aus, dass das Unternehmen den Beschwerdeführer wegen fehlender Datensicherheitsmaßnahmen (Art. 32 DSGVO) – konkret wegen eines fehlenden „Double-Opt-In-Verfahrens“ – in seinem Recht auf Geheimhaltung gemäß § 1 Absatz 1 DSG verletzt hat.

Beim „Double-Opt-In-Verfahren“ gibt ein User die Zustimmung zur Verwendung seiner personenbezogenen Daten doppelt („double“): Zunächst meldet sich der User auf der Website des Unternehmens, dessen Services er nutzen will, mit seiner E-Mail-Adresse an. Danach schickt ihm das Unternehmen auf die angegebene E-Mail-Adresse ein Bestätigungs-E-Mail. Erst wenn der User seine Anmeldung - etwa durch Anklicken eines Aktivierungslinks im Bestätigungs-E-Mail - nochmals bestätigt, hat das Unternehmen eine DSGVO-konforme Zustimmung zur Verwendung der personenbezogenen Daten des Users erlangt.

Im vorliegenden Fall reichte die Bekanntgabe einer beliebigen E-Mail-Adresse, um sich bei den Onlinedating-Portalen des Unternehmens anzumelden. Das Unternehmen schickte dem User zwar ein Bestätigungs-E-Mail an die angegebene E-Mail-Adresse, wartete aber nicht darauf, dass der User seine Anmeldung nochmals durch Anklicken eines Aktivierungslinks im Bestätigungs-E-Mail bestätigte. Das Unternehmen verwendete also kein „Double-Opt-In-Verfahren“, vielmehr erlaubte es dem User, der sich auf der Website des Unternehmens anmeldete, sofort – das heißt mit Bekanntgabe der E-Mail-Adresse – die Nutzung seiner Onlinedating-Portale. Das führte - wie im vorliegenden Beschwerdefall - dazu, dass eine fremde Person die E-Mail-Adresse

des Beschwerdeführers dazu nutzte, sich für die Onlinedating-Portale des Unternehmens anzumelden, sodass diese fremde Person sofort die Onlinedating-Portale des Unternehmens selbst nutzen konnte und der Beschwerdeführer auf seine E-Mail-Adresse Sex-Spams erhielt, ohne sich jemals auf dessen Onlinedating-Portalen angemeldet zu haben.

Der Bescheid ist rechtskräftig.

31. Bescheid vom 10.10.2019, GZ: DSB-D124.1078/0002-DSB/2019 (Identität der Sache, Beschwerde unzulässig bei rechtskräftigem Gerichtsurteil, kein Recht auf Verwaltungsstrafverfahren, RIS)

In dieser Sache hatte sich die Datenschutzbehörde mit der Frage zu befassen, ob gegen die Videoüberwachung eines Nachbarn eine Beschwerde gemäß Art. 77 DSGVO und § 24 DSG zulässig bleibt, wenn bereits ein rechtskräftiges Unterlassungsurteil eines Bezirksgerichts gegen den Nachbarn ergangen ist.

Die Datenschutzbehörde kam hier zu dem Schluss, auch wenn Art. 77 und Art. 79 DSGVO den Anschein erwecken, dass eine parallele oder sukzessive Verfahrensführung vor einer Aufsichtsbehörde und einem Gericht möglich scheint, es nicht der Zweck der DSGVO sein kann, zunächst ein Gericht mit der Frage der Rechtmäßigkeit einer bestimmten Verarbeitung personenbezogener Daten zu befassen, nur um dieselbe Frage nach Abschluss des Rechtszuges der Beantwortung einer Aufsichtsbehörde für Datenschutz zuzuführen. Das Unterlassungsurteil bildet einen vollstreckbaren Titel. Eine sukzessive Inanspruchnahme der Datenschutzbehörde in derselben Sache kommt nicht in Betracht, zumal dem Rechtsschutzbedürfnis der Beschwerdeführer durch das Urteil bereits vollumfänglich Rechnung getragen wurde. Eine Beschwerde ist daher nicht mehr anzunehmen; die Beschwerde wurde daher zurückgewiesen.

Ebenfalls zurückgewiesen wurde der Antrag auf Verhängung einer Geldbuße gegen den Nachbarn, weil Verwaltungsstrafverfahren wegen Verstößen gegen die DSGVO ausschließlich von Amts wegen einzuleiten sind.

Dieser Bescheid ist rechtskräftig.

32. Bescheid vom 11.10.2019, GZ: DSB-D124.1456/0003-DSB/2019 (Berichtigung, kein Recht auf Berichtigung von Bescheidinhalten, nicht rechtskräftig)

Der Beschwerdeführer hatte die Mitteilung einer Staatsanwaltschaft erhalten, wonach ein gegen ihn geführtes Ermittlungsverfahren gemäß § 190 Z 1 StPO eingestellt wurde.

Er verlangte daraufhin, gestützt auf § 45 Abs. 1 DSG, die Berichtigung/Abänderung zweier Passagen eines Bescheids des Bundesministers für Inneres, die von ihm geltend gemachte Entschädigungsansprüche nach dem Polizeibefugnis-Entschädigungsgesetz (PolBEG) betrafen, dahingehend, dass er das ihm vorgeworfene Verhalten gar nicht gesetzt habe, und dass ihm bei den gegen ihn gesetzten Amtshandlungen ein Schaden entstanden sei. Außerdem beantragte er die Berichtigung seines fehlerhaft angeführten akademischen Grades.

Der Beschwerdegegner reagierte zunächst nicht auf diesen Antrag und brachte erst nach Einbringung einer Beschwerde bei der Datenschutzbehörde vor, der Inhalt der Erledigung sei richtig wiedergegeben, diese könne aber nicht angefochten werden.

Die Datenschutzbehörde führte in ihren rechtlichen Erwägungen aus, § 45 und das 3. Hauptstück des DSG (bzw. die DSRL-PJ) würden hier nicht zur Anwendung kommen. Die entspre-

chenden Daten seien für den Zweck der Beurteilung von Entschädigungsansprüchen des Beschwerdeführers verarbeitet worden. Dies falle nicht in den Anwendungsbereich der DSRL-PJ.

Die Abänderung eines Bescheids der in der Sache zuständigen Behörde durch einen Bescheid der Datenschutzbehörde sei nicht möglich. Der Bescheid hätte inhaltlich mit den vorgesehenen Rechtsbehelfen (Anrufung des zuständigen Gerichts gemäß § 9 Abs. 2 PolBEG) bekämpft werden müssen. Die Schreibweise des akademischen Grads sei nur geringfügig unrichtig, die Gefahr einer Verwechslung bestehe nicht.

Die Beschwerde wurde daher abgewiesen.

Dieser Bescheid ist nicht rechtskräftig.

33. Bescheid vom 8.11.2019, GZ: DSB-D122.970/ 0004-DSB/2019 (Löschung eines pseudonymen Nutzerprofils, rechtskräftig, Newsletter 1/2020, Seite 4, RIS)

In dieser Sache hatte sich die DSB mit der Verarbeitung pseudonymisierter Daten (Art. 4 Z 5 DSGVO) zu befassen. Der Beschwerdeführer hatte beim Anbieter eines Internet-Kleinanzeigenportals ein Nutzerprofil angelegt, das nur durch einen (wählbaren) Nutzernamen und eine E-Mail-Adresse als „unique identifier“ gekennzeichnet war. Dieses Nutzerprofil wollte er nun löschen lassen. Eine Möglichkeit zur Selbstlöschung wurde nicht angeboten. Das verantwortliche Unternehmen reagierte auf den per E-Mail gesendeten Löschungswunsch mit der Aufforderung, einen umfassenden Löschungsantrag auszufüllen und darin u.a. den vollständigen (Real-) Namen und die Wohnadresse bekanntzugeben. Die Datenschutzbehörde gab der Beschwerde Folge, stellte eine Verletzung des Löschungsrechts fest und trug der Beschwerdegegnerin auf, das Profil zu löschen. Begründet wurde dies u.a. mit einem Verstoß gegen die Pflicht gemäß Art. 12 Abs. 2 DSGVO, der betroffenen Person die Ausübung ihrer Rechte zu erleichtern, und der fehlenden Möglichkeit, die im verlangten Löschungsantrag zusätzlich erhobenen Daten zwecks Feststellung der Identität mit bereits verarbeiteten Daten zu vergleichen. Bei einem pseudonymen Nutzerprofil reiche es aus, wenn sich der Nutzer etwa durch Kenntnis der Login-Daten (User-ID, Passwort), durch Angaben zum gespeicherten Dateninhalt des Profils oder durch die nachgewiesene Verfügungsgewalt über die Mailbox, deren E-Mail-Adresse anlässlich der Registrierung angegeben worden ist, identifizieren könne.

Dieser Bescheid ist rechtskräftig.

34. Bescheid vom 2.12.2019, GZ: DSB-D124.352/0003-DSB/2019 (Facebook-Postings zu Polizeieinsatz, Abwägung zwischen den Rechten auf Geheimhaltung und freie Meinungsäußerung, nicht rechtskräftig, Newsletter 1/2020, Seite 3)

In diesem Bescheid hatte sich die Datenschutzbehörde mit einer Abwägung des Rechts auf Geheimhaltung (§ 1 DSG) gegen das Recht auf freie Meinungsäußerung auseinander zu setzen.

Die Beschwerdeführerin ist Polizistin in Tirol und war Teil eines Einsatzes zur Weihnachtszeit 2018. Ein 12-jähriger Minderjähriger – untergebracht in einem Wohnheim – war abgängig. Er hatte seine Familie und zwei Schwestern zu Weihnachten 2018 - besucht. Die Eltern hatten aufgrund der bekannten Abgängigkeit im Wohnheim die Polizei verständigt, die – von der Bezirksleitstelle beauftragt – mit zwei Streifenwagen und 6 Mann uniformierter Besatzung bei dem Einfamilienhaus vorgefahren war, um den Minderjährigen abzuholen.

Der Vater des Minderjährigen – Beschwerdegegner des Verfahrens vor der Datenschutzbehörde - hatte vom Dachgeschoß aus Fotos angefertigt, die die in der Auffahrt geparkten Einsatzfahrzeuge samt

mehreren Polizisten zeigten und auf Facebook mit dem Zusatz „So werden 12jährige Kinder mit der Polizei gegen ihren Willen von zuhause weggezogen. Bitte teilen“ gepostet.

Die Beschwerdeführerin forderte daraufhin den Beschwerdegegner telefonisch auf, das Facebook-Posting zu entfernen. Kurz darauf veröffentlichte der Beschwerdegegner nochmals dieselben Fotos auf Facebook, diesmal unter dem Titel „Auf ein neues Frau Müller“ (Name der Beschwerdeführerin von der Datenschutzbehörde geändert).

Die Beschwerdeführerin fühlte sich durch die beiden Facebook-Postings in ihrem Recht auf Geheimhaltung verletzt.

Die Datenschutzbehörde wies die Beschwerde hinsichtlich des ersten Postings ab, weil davon auszugehen war, dass damit ein Beitrag zu einer Debatte von öffentlichem Interesse (namentlich die Angemessenheit der Abholung Minderjähriger mit zwei Streifenwägen und 6 Mann uniformierter Besatzung) vorlag und das Recht auf freie Meinungsäußerung überwog.

Anders stellte sich der Sachverhalt in Bezug auf das zweite Posting dar: Dieses Posting lieferte keinen Beitrag zu einer Debatte im öffentlichen Interesse. Der Beschwerdegegner bezweckte damit vielmehr seinem Unmut öffentlich Ausdruck zu verleihen und nannte zudem auch noch den Nachnamen der Beschwerdeführerin, weswegen das schutzwürdige Geheimhaltungsinteresse der Beschwerdeführerin überwog und der Beschwerde in diesem Punkt stattzugeben war.

Dieser Bescheid ist nicht rechtskräftig.

Österreichische Post AG

Durch einen Anfang Jänner 2019 veröffentlichten Artikel der Plattform „Addendum“ wurde bekannt, dass die Österreichische Post AG in großem Umfang mit Marketingdaten handelt. Dabei wurden Daten wie Name, Adresse, Geschlecht und Alter mit errechneten Wahrscheinlichkeitswerten verknüpft und zum Verkauf angeboten. Insbesondere die Berechnung und Verknüpfung von „Parteiaffinitäten“ zu konkreten personenbezogenen Daten Betroffener führte zu großer medialer Aufmerksamkeit.

Eigenen Angaben zufolge erhielt die Österreichische Post AG aufgrund der Berichterstattung über den Adresshandel über 10.000 Auskunftersuchen. Im Jahr 2019 wurden in der Folge diese Thematik betreffend mehr als 500 Individualbeschwerden bei der Datenschutzbehörde anhängig gemacht. Die Individualbeschwerden bei der Datenschutzbehörde betreffen überwiegend behauptete Verletzungen im Recht auf Auskunft und im Recht auf Geheimhaltung. Anfangs wurden großteils Beschwerden betreffend das Recht auf Auskunft aufgrund einer behaupteten Nichterteilung der Auskunft bzw. einer behaupteterweise mangelhaften Erteilung der Auskunft anhängig gemacht, gegen Jahresende nahm die Zahl der Beschwerden betreffend das Recht auf Geheimhaltung, insbesondere bezüglich der Berechnung der „Parteiaffinitäten“ durch die Beschwerdegegnerin, stark zu.

Von den Verfahren vor der Datenschutzbehörde konnten bisher bereits mehr als 150 Verfahren gemäß § 24 Abs. 6 DSGVO eingestellt werden, da die Beschwerdegegnerin im Verfahren die Auskunft nachträglich erteilte und die Betroffenen die verfahrensgegenständliche Auskunft erhielten.

3.2.1.2 Grenzüberschreitende Fälle der DSB¹

Im Jahr 2019 wurden bei der DSB 95 Beschwerdefälle eingebracht, die einen grenzüberschreitenden Sachverhalt iSd Art. 4 Z 23 DSGVO aufwiesen. Darüber hinaus waren 2019 bei der DSB 917 grenzüberschreitende Fälle anhängig, die seit dem 25. Mai 2018 an die Datenschutzbehörde von einer anderen Aufsichtsbehörde herangetragen wurden.

Die DSB führte seit 25. Mai 2018 14 Verfahren als federführende Aufsichtsbehörde gegenüber einem Verantwortlichen, wobei den anderen betroffenen Aufsichtsbehörden iSd Art. 4 Z 22 DSGVO seitens der DSB im Jahr 2019 in 4 Verfahren ein Beschlussentwurf gemäß Art. 60 Abs. 3 DSGVO vorgelegt wurde. Zwei dieser Verfahren betrafen Verletzungen im Recht auf Auskunft bzw. Löschung, die im laufenden Verfahren beseitigt wurden. In einem weiteren Beschwerdefall wegen einer Verletzung des Art. 6 DSGVO betreffend eine behauptete rechtswidrige Bonitätsanfrage eines österreichischen Verantwortlichen wurde die Beschwerde durch die Beschwerdeführerin zurückgezogen. Im vierten Verfahren erfolgte die beanstandete Löschung bereits zeitlich vor Einbringung der Beschwerde bei der initiierenden Aufsichtsbehörde, weshalb ein subjektives Rechtsschutzbedürfnis seitens der DSB verneint wurde.

Im Rahmen der grenzüberschreitenden Zusammenarbeit innerhalb und außerhalb eines konkreten Verfahrens machte die DSB seit 25. Mai 2018 80 Mal von der gegenseitigen Amtshilfe iSd Art. 61 DSGVO Gebrauch und wurde selbst in 110 Fällen von anderen Aufsichtsbehörden kontaktiert.

Insgesamt wurden seit dem 25. Mai 2018 von allen Aufsichtsbehörden 142 Beschlussentwürfe iSd Art. 60 Abs. 3 DSGVO vorgelegt, die in 82 finalen Beschlüssen iSd Art. 60 Abs. 6 DSGVO mündeten.

Bisher wurde dem EDSA kein einziges grenzüberschreitendes Verfahren zur Streitbeilegung iSd Art. 65 Abs. 1 lit. a bzw. b DSGVO in Vorlage gebracht.

Der DSB obliegt die Zuständigkeit zur Verfahrensführung auch in jenen Fällen, in denen ein Verantwortlicher zwar über keine Niederlassung in der Union iSd Art. 56 Abs. 1 DSGVO verfügt, die Datenverarbeitung jedoch gemäß Art. 3 Abs. 2 DSGVO in den Anwendungsbereich der DSGVO fällt. In solchen Fällen führt die DSB das Verfahren grundsätzlich eigenständig mit dem betreffenden Verantwortlichen im Drittstaat bzw. mit dessen Vertreter im Unionsgebiet gemäß Art. 4 Z 17 iVm Art. 27 DSGVO. So behandelte die DSB 2019 den Fall² einer behaupteten Verletzung im Grundrecht auf Datenschutz durch Versenden einer E-Mail zu Werbezwecken ohne entsprechende Einwilligung des Beschwerdeführers seitens eines ausschließlich in den USA niedergelassenen Verantwortlichen. Die Verarbeitung der Daten des in Österreich wohnhaften Beschwerdeführers stand im Zusammenhang mit dem Anbieten von Waren bzw. Dienstleistungen (Angebot zur Teilnahme an einer Eventveranstaltung in Deutschland), weshalb der räumliche Anwendungsbereich der DSGVO gemäß Art. 3 Abs. 1 lit. a DSGVO eröffnet war. Die DSB stellte hierbei auf Grund eines Verstoßes gegen die e-Datenschutz-RL (RL 2002/58/EG) eine Verletzung von § 1 Abs. 1 DSG iVm Art. 8 Abs. 1 EU-GRC fest.

1 Eine umfassende Darlegung des One-Stop-Shop Verfahrens bzw. des Kooperationsmechanismus gemäß Art. 56 und 60 DSGVO ist dem Datenschutzbericht 2018, Kapitel 3.2.1.2 zu entnehmen.

2 Bescheid der DSB vom 7. März 2019, DSB-D130.033-DSB/2019: https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=d9ca6696-3b8b-45af-9bc8-a43831ad474d&Position=1&SkipToDocumentPage=True&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=False&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=05.02.2020&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20190307_DSB_D130_033_0003_DSB_2019_00

Ein anderer von der DSB behandelter Fall³ betraf eine behauptete Verletzung im Recht auf Information gemäß Art. 13 DSGVO durch eine Hotelbuchungsplattform, die für Zwecke eines Verantwortlichen mit einzigem Sitz in der Schweiz betrieben wurde. Da die gegenständliche Verarbeitung der personenbezogenen Daten des in Österreich wohnhaften Beschwerdeführers ebenfalls in Zusammenhang mit dem Anbieten von Waren bzw. Dienstleistungen (Betrieb einer deutschen Buchungsplattform unter einer österreichischen Toplevel-Domain) stand, fand gemäß Art. 3 Abs. 2 lit. a DSGVO auch hier die DSGVO Anwendung. Der Beschwerde wurde zum Teil stattgegeben und eine Verletzung im Recht auf Information gemäß Art. 13 DSGVO festgestellt.

3.2.2 Rechtsauskünfte an Bürgerinnen und Bürger

Die Datenschutzbehörde stellt auf ihrer [Webseite](#) umfassende Informationen im Zusammenhang mit dem geltenden Datenschutzrecht zur Verfügung. Hierbei handelt es sich um Antworten auf die relevantesten datenschutzrechtlichen Fragen. Kürzlich überarbeitet wurden unter anderem die Fragen und Antworten zu Dashcams und zur Videoüberwachung.

Darüber hinaus finden sich auf der [Webseite](#) der Datenschutzbehörde ausführliche Informationen über die Rechte der betroffenen Personen und die Zuständigkeit der Datenschutzbehörde. Der [Leitfaden zur DSGVO](#) wird laufend aktualisiert.

Darüber hinaus beantwortet die Datenschutzbehörde allgemeine Anfragen zum geltenden Datenschutzrecht schriftlich. Telefonische Rechtsauskünfte werden nicht erteilt. Die Datenschutzbehörde nimmt im Rahmen der Beantwortung von Anfragen grundsätzlich keine Vorabprüfung hinsichtlich der Unzulässigkeit/Zulässigkeit einer bestimmten Datenverwendung, der Anwendung bzw. Auslegung rechtlicher Bestimmungen oder einer sonstigen inhaltlichen Anfrage vor, da jede Antwort ein entsprechendes, vom Gesetz vorgesehenes Verfahren vor der Datenschutzbehörde, präjudizieren würde.

3.2.3 Genehmigungen im Internationalen Datenverkehr

Eine große Änderung mit Einführung der Datenschutz-Grundverordnung (DSGVO) war die weitgehende Genehmigungsfreiheit für internationalen Datenverkehr an Empfänger außerhalb des EWR.

Die DSGVO regelt die Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen in Kapitel V. Alle bisher bekannten rechtlichen Instrumente stehen nach wie vor zur Verfügung. Nur gemäß Art. 46 Abs. 3 DSGVO ist in bestimmten Fällen eine Genehmigung durch die zuständige Aufsichtsbehörde vorgesehen. Im Jahr 2019 wurde ein einziger Fall gemäß Art. 46 Abs. 3 lit. a DSGVO bei der DSB anhängig gemacht.

Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules – BCRs) müssen gemäß Art. 63 ff DSGVO durch die zuständige Aufsichtsbehörde genehmigt werden. Hierbei ist eine enge Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss notwendig⁴. Die federführende Aufsichtsbehörde übernimmt dabei die Kommunikation mit dem Antragsteller, hat aber gleichzeitig die Kommentare und

3 Bescheid der DSB vom 22. August 2019, DSB-D130.206/0006-DSB/2019: https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=79e77c28-ef2d-4e8f-9f81-774e459631ce&Position=1&SkipToDocumentPage=True&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=False&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=05.02.2020&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20190822_DSB_D130_206_0006_DSB_2019_00.

4 Das Prozedere ist im Arbeitsdokument WP263 rev.01 der ehemaligen Artikel-29-Datenschutzgruppe beschrieben.

Anmerkungen aller anderen Aufsichtsbehörden zu berücksichtigen. Der finale Entwurf muss dem Europäischen Datenschutzausschuss vorgelegt werden, welcher über die Annahme des Entwurfs abstimmt.

Bei der Datenschutzbehörde wurden im Jahr 2019 lediglich drei BCR-Genehmigungsverfahren anhängig gemacht.

Aufgrund der Komplexität von BCRs sollte im ersten Schritt immer nach der Notwendigkeit von BCRs gefragt werden. Insbesondere sollte abgewogen werden, ob die Zulässigkeit der Datenübermittlung an Drittländer nicht einfacher und effizienter durch andere geeignete Garantien iSd Art. 46 Abs. 2 DSGVO erreicht werden kann (z.B. Standarddatenschutzklauseln). Das ist insbesondere dann empfehlenswert, wenn die Anzahl der Unternehmenstöchter in Drittstaaten gering ist. BCRs sollten immer nur dann zum Einsatz kommen, wenn die Nutzung anderer geeigneter Garantien problematisch erscheint.⁵

3.2.4 Genehmigungen nach §§ 7 u. 8 DSG

Allgemeines

§ 7 DSG regelt die Voraussetzungen der Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archiv-, wissenschaftliche, historische, oder statistische Zwecke.

§ 8 DSG regelt die Bedingungen für die Zurverfügungstellung von Adressdaten zum Zwecke der Benachrichtigung / Befragung aus einem wichtigen Interesse des Betroffenen selbst, aus einem wichtigen öffentlichen Benachrichtigungs- und Befragungsinteresse oder zur Befragung der betroffenen Personen für wissenschaftliche oder statistische Zwecke.

Entscheidungen der Datenschutzbehörde im Jahr 2019

Die Datenschutzbehörde hat im Jahr 2019 achtzehn Bescheide im Rahmen von §§ 7,8 DSG getroffen, davon vier Zurückweisungen (zwei wegen der Genehmigungsfreiheit des § 8 Abs. 2 Z 1 DSG (Beeinträchtigung der Geheimhaltungsinteressen unwahrscheinlich und Verarbeitung der Daten durch denselben Verantwortlichen), eine Zurückweisung wegen § 7 Abs. 3 Z. 1 DSG (Vorliegen der Einwilligung) und eine Zurückweisung gemäß § 13 Abs. 3 AVG).

15 Entscheidungen betrafen Genehmigungen gemäß § 7 DSG zu Forschungszwecken.

Ein Großteil der Genehmigungen gemäß § 7 DSG zu Forschungszwecken kann direkt oder indirekt dem Straßenverkehr zugeordnet werden (etwa Forschungen im Rahmen von Kollisionserkennungssystemen (DSB-D202.221/0001-DSB/2019), automationsunterstützte Identifizierung von riskanten Straßenabschnitten für Motorradfahrer (DSB-D202.236/0001-DSB/2019), Erforschung zur Nutzung des öffentlichen Straßenraums durch unterschiedliche Verkehrsteilnehmer (DSB-D202.229/0003-DSB/2019), automatisiertes Fahren (DSB-D202.232/0001-DSB/2019, DSB-D202.220/0002-DSB/2019) sowie Systeme zur automationsunterstützten Erkennung von Kennzeichentafeln zur Parkplatzgebührenverrechnung (DSB-D202.228/0002-DSB/2019).

Ein Bescheid betraf die Genehmigung zur Erfassung und Analyse personenbezogener Daten bei Infektionen in Gesundheitseinrichtungen (DSB-D202.222/0002-DSB/2019), ein weiterer Bescheid befasste sich mit der Entwicklung einer Software im Rahmen des - von der Europäischen Union - geförderten Projektes Copkit zur Aufbereitung und Verknüpfung großer Datenmengen

⁵ Vgl. hierzu WP 74 der Artikel-29-Datenschutzgruppe

im Rahmen eines Frühwarnsystems zur Bekämpfung von Terrorismus und organisiertem Verbrechen (DSB-D202.224/0002-DSB/2019).

3.2.5 Amtswegige Prüfverfahren

Die DSB hat im Jahr 2019 215 amtswegige Verfahren eingeleitet; 88 amtswegige Verfahren wurden im Berichtszeitraum mit Einstellung und 15 mit Bescheid, sohin 103 Verfahren gesamt abgeschlossen.

Ausgewählte Verfahren:

Neben den amtswegigen Verfahren, die aufgrund anonymer Eingaben (überwiegend zur Überprüfung der Rechtmäßigkeit von Bildaufzeichnungsanlagen – Videoüberwachungen im privaten Bereich), Eingaben durch Behörden oder auf Eigeninitiative der Datenschutzbehörde erfolgen, führt die Datenschutzbehörde seit 2014 jährlich Schwerpunktverfahren durch. Dabei wird ein bestimmter Sektor einer eingehenden datenschutzrechtlichen Überprüfung – einschließlich Vorortuntersuchungen – unterzogen. Im Jahr 2019 wurde – bedingt durch die anhaltend hohe Belastung nach in Geltung treten der DSGVO und dem damit verbundenen generellen Anstieg an Verfahrenszahlen – wie im davorliegenden Berichtszeitraum kein Schwerpunktverfahren durchgeführt.

Ausgewählte Entscheidungen:

D213.895 (Einwilligung ins Profiling)

Die Datenschutzbehörde hat gegen den Verantwortlichen einer Vorteilskarte ein Prüfverfahren eingeleitet, weil Bedenken betreffend die Rechtmäßigkeit der Rechtsgrundlage zur Datenverarbeitung bestanden. Der Verantwortliche betreibt mit Kundendaten, bestehend aus Mitglieder-stammdaten, Teilnahmedaten, Einkaufsdaten und Marketing-Profilingdaten eine ausführliche Datenanalyse zum Zwecke der Gewinnung von Daten mittels Profiling. Als Rechtsgrundlage wurde die datenschutzrechtliche Einwilligung genannt, die unterschiedlich eingeholt wurde, je nachdem ob die betroffene Person in der Filiale eines teilnehmenden Unternehmens, auf der Homepage der Verantwortlichen oder in der eigenen App ihre Zustimmung erteilte. Die Datenschutzbehörde hat dazu gemäß den von der ständigen Rechtsprechung getragenen Grundsätzen zur Freiwilligkeit, Bestimmtheit, Information, Verständlichkeit, leichten Zugänglichkeit, klare und einfache Sprache ausgesprochen, die geprüfte Datenanwendung entspreche nicht gesetzlichen Erfordernissen und sei die Einwilligung daher ungültig. Demnach könne eine betroffene Person insbesondere nicht klar erkennen wozu eine Einwilligung abgegeben werde, die Informationen über das Bestehen des Widerrufsrechts seien unzureichend und, dass insgesamt aus Sicht einer betroffenen Person der Eindruck entstehe, dass die Datenverarbeitung zum Zwecke des Erwerbs von Gutscheinen erfolge, wobei das Profiling des Kunden tatsächlich im Vordergrund stünde. Es sei deshalb – als Rechtfertigungsgrund kämen auch überwiegende Interessen des Verantwortlichen nicht infrage – die Datenverarbeitung des Profiling ohne gültige Rechtsgrundlage rechtswidrig.

Der Bescheid der Datenschutzbehörde ist nicht in Rechtskraft erwachsen, einer Beschwerde- vorentscheidung folgend, wurde die Vorlage zum Bundesverwaltungsgericht beantragt

D213.864 (Biometrische Daten - Venenscan)

Der Betreiber eines Strandbades hat zwecks Zutrittskontrolle biometrische Daten mittels Handvenenscan erhoben. Die Datenschutzbehörde leitete dazu ein amtswegiges Prüfverfahren ein und definierte als Prüfgegenstand die Rechtmäßigkeit der Datenverarbeitung. Der Betreiber hat seit Mai 2019 Saisonkartenbesitzer dazu verpflichtet, ein Scanmuster der handinnenliegenden Venen abzugeben, damit beim Zutritt zum Strandbad mittels biometrischen Mustern die Identität bestätigt werden kann. Als Rechtsgrundlage diene eine verpflichten-

de datenschutzrechtliche Einwilligungserklärung. Die Datenschutzbehörde sprach dazu aus, dass die Verarbeitung biometrischer Daten einem Verarbeitungsverbot unterliege und nur mit der expliziten Einwilligung einer betroffenen Person verarbeitet werden dürfe. Die vom Verantwortlichen eingeholte Einwilligung stelle sich aber als rechtswidrig heraus und sei daher ungültig: die Einwilligung komme nicht freiwillig zustande und sei darüber hinaus an die Vertragserfüllung gekoppelt. Im Effekt habe eine betroffene Person keine Wahl als zuzustimmen, obwohl es für den Zugang nicht zwingend erforderlich sei, biometrische Daten zu erheben und sei die Einwilligung daher ungültig. Auch sei die Datenverarbeitung unverhältnismäßig, weil derselbe Informationsgehalt auch mit gelinderen Mitteln zu erheben wäre. Das amtswegige Verfahren sei daher berechtigt gewesen und die Datenverarbeitung nicht rechtskonform.

Die Entscheidung ist rechtskräftig.

3.2.6 Beschwerdeverfahren vor dem Bundesverwaltungsgericht einschließlich Säumnisbeschwerden

Im Berichtszeitraum wurden 164 Beschwerden gegen Bescheide der Datenschutzbehörde erhoben.

Es gab 31 Säumnisbeschwerden im Jahr 2019.

W258 2201288-1, Erkenntnis vom 3. April 2019

Das Bundesverwaltungsgericht hat einer Beschwerde gegen den Bescheid der Datenschutzbehörde vom 1. Juni 2018, GZ DSB D213.600/0001-DSB/2018, mit Erkenntnis vom 3. April 2019 teilweise Folge gegeben.

Im - noch nach § 30 DSG 2000 eingeleiteten - Prüfverfahren hatte die Datenschutzbehörde zusammengefasst festgestellt, dass die Übergabe von Patientenkarteien an eine Kassenärztin, die nicht Kassenplanstellennachfolgerin oder Ordinationsstättennachfolgerin ist (vgl. § 51 ÄrzteG), eine Rechtsverletzung darstellt und ordnete die Übergabe der ärztlichen Dokumentation an die Kassenplanstellennachfolgerin an. Dagegen erhoben der die Patientenkarteien weitergebende Arzt (Erstbeschwerdeführer) sowie die Ärztin, die die Patientendaten erhalten hat, (Zweitbeschwerdeführerin) Beschwerde.

Das Bundesverwaltungsgericht kam zum Schluss, dass die Datenschutzbehörde die Rechtswidrigkeit der Übergabe der Patientendaten zu Recht festgestellt hat. Die Datenschutzbehörde bezog sich in ihrem Bescheid jedoch auf alle ehemaligen Patienten des Erstbeschwerdeführers. Das Bundesverwaltungsgericht hat einen Spruchpunkt dahingehend eingeschränkt, dass nur jene Patienten in ihrem Recht auf Geheimhaltung verletzt seien, deren Patientendaten tatsächlich übergeben worden sind. Es bestand nämlich für die Patienten die Möglichkeit, der Übergabe der Patientenkarteien zu widersprechen. Im Falle eines solchen Widerspruchs wurden die Daten dieser Patienten nicht weitergegeben.

Betreffend den Leistungsauftrag der DSB, wonach die ärztliche Dokumentation der Kassenplanstellennachfolgerin übergeben werden muss (Spruchpunkt 2. des bekämpften Bescheides), führte das Bundesverwaltungsgericht aus, § 51 Abs. 4 ÄrzteG stelle keine taugliche Rechtsgrundlage dar, um den Erstbeschwerdeführer zur Übergabe seiner Patientenkartei an den Kassenplanstellennachfolger zu verpflichten, weshalb der Spruchpunkt abgeändert wurde.

Diese Entscheidung ist nicht rechtskräftig.

W214 2207491-1, Erkenntnis vom 4. April 2019

Das Bundesverwaltungsgericht hat mit Erkenntnis vom 4. April 2019, GZ W214 2207491-1, die Beschwerdeentscheidung der DSB vom 18. September 2018, GZ: DSB-D062.151/0001-DSB/2018, ersatzlos behoben.

Im amtswegigen Prüfverfahren nach Art. 58 Abs. 1 lit. b DSGVO hat die Datenschutzbehörde zusammengefasst festgestellt, dass die Einholung der Einwilligung des Verantwortlichen (Arbeitgeber) für den Einsatz eines GPS-Trackers an Firmenfahrzeugen von den Betroffenen (Arbeitnehmern) nicht freiwillig erfolgt und dass der Verantwortliche die Verarbeitung (Nutzung des GPS-Systems für firmeneigene Fahrzeuge) in Einklang mit der DSGVO bringen möge. Das Bundesverwaltungsgericht hat zusammengefasst ins Treffen geführt, dass die Datenschutzbehörde den Prüfgegenstand zu eng definiert und etwa nicht überprüft habe, ob auch eine weitere Rechtsgrundlage – insbesondere berechtigte Interessen nach Art. 6 Abs. 1 lit. f DSGVO – in Betracht käme.

Die Datenschutzbehörde hat dagegen außerordentliche Revision an den Verwaltungsgerichtshof erhoben.

W258 2205602-1, Erkenntnis vom 24. Mai 2019

Die Datenschutzbehörde hat in einem 2018 geführten Verfahren gegen ein Geldinstitut entschieden, dass bei einem datenschutzrechtlichen Auskunftsbegehren die Vergebührung von Kontoauszügen, welche nicht mehr elektronisch abrufbar sind, unzulässig ist.

Im zugrundeliegenden Fall hatte das Geldinstitut die Herausgabe von Kontoauszügen an Gebühren nach dem ZaDiG 2018 geknüpft. Das Auskunftsbegehren nach dem damaligen § 26 DSG 2000 wurde nicht inhaltlich beantwortet. Das Verfahren ging in der Folge über den 25. Mai 2018 hinaus und war nach der neuen Rechtslage zu entscheiden. Die Datenschutzbehörde erkannte dabei, dass die dem DSG 2000 immanente Subsidiarität des datenschutzrechtlichen Auskunftsrechts gegenüber anderen gesetzlichen Einsichtsrechten nicht auch durch Art. 15 DSGVO abgebildet wird und demnach grundsätzlich kostenfrei gewährt werden muss. Das Geldinstitut berief sich auf die Rechtmäßigkeit der Gebühren nach dem ZaDiG 2018, da es datenschutzrechtliche Spezialnormen enthalte. Dem folgte die Datenschutzbehörde nicht.

Das Bundesverwaltungsgericht bestätigte mit Erkenntnis vom 24. Mai 2019 die Entscheidung der Datenschutzbehörde mit der Maßgabe, dass die vom Geldinstitut genannten Bestimmungen keine das Auskunftsrecht nach Art. 15 DSGVO spezielleren Normen beinhalten, sondern den Informationspflichten Art. 13 und 14 DSGVO gleichen.

Diese Entscheidung ist rechtskräftig.

W214 2219944-1, Erkenntnis vom 3. September 2019

Das Bundesverwaltungsgericht hat mit Erkenntnis vom 3. September 2019 den Bescheid der Datenschutzbehörde vom 24. April 2019, GZ DSB-D124.273/0003-DSB/2019, bestätigt und die Beschwerde als unbegründet abgewiesen. Im Beschwerdeverfahren vor der Datenschutzbehörde wurde festgestellt, dass der Verantwortliche die Beschwerdeführerinnen dadurch im Recht auf Geheimhaltung verletzt hat, indem dieser Videoaufnahmen von den Beschwerdeführerinnen ohne deren Wissen angefertigt hat, während sich diese nach dem Fußballtraining nackt in der Dusche befunden haben.

Das Bundesverwaltungsgericht führte aus, dass eine Duschkabine jedenfalls zum höchstpersönlichen Lebensbereich zählt und eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO gegen den Verantwortlichen ausschlägt. Der seitens des Verantwortlichen ins Treffen geführte

Umstand, dass dieser die Videoaufnahmen nicht angesehen habe, sei nicht zu berücksichtigen, da das Konzept der DSGVO keine „Mindestverarbeitung“ bzw. „Mindestverwendung“ kennt, der Begriff der Verarbeitung gemäß Art. 4 Z 2 DSGVO also bereits durch das Anfertigen von Videoaufnahmen erfüllt ist.

Dieses Erkenntnis ist rechtskräftig.

W211 2209492-1, Erkenntnis vom 18. Dezember 2019

Mit Erkenntnis vom 18. Dezember 2019 hat das Bundesverwaltungsgericht einer Beschwerde gegen den Bescheid der Datenschutzbehörde, GZ DSB-D123. 204/0005-DSB/2018, stattgegeben und den Bescheid ersatzlos behoben.

Zusammenfasst hat die Datenschutzbehörde festgestellt, dass es sich beim Betrieb eines digitalen Türspions um eine Bildaufnahme iSd § 12 Abs. 1 DSG handelt und unter Hinweis auf die Judikatur des Obersten Gerichtshofes ausgeführt, dass der verfahrensgegenständliche Türspion in einem Mehrparteienhaus aufgrund der unmittelbaren Nähe der Wohnungseingangstüren den höchstpersönlichen Lebensbereich des Beschwerdeführers aufnehme und dass aufgrund der mangelnden Einwilligung der betroffenen Person, die Bildaufnahme unzulässig sei. Gleichzeitig wurde die Datenverarbeitung durch den digitalen Türspion mit sofortiger Wirkung untersagt.

Das Bundesverwaltungsgericht hielt, wie bereits in zwei vorangehenden Entscheidungen (siehe dazu Beschluss vom 20.11.2019, W256 2214855-1, und Erkenntnis vom 25.11.2019, W211 2210458-1), fest, dass für die Anwendung der §§ 12 und 13 DSG mangels entsprechender Öffnungsklausel in der DSGVO kein Raum bestehe und diese daher unangewendet (vgl. EuGH, 09. 03. 1977, C-106/77) zu bleiben haben und der Fall daher auf Basis der DSGVO zu prüfen sei.

Die Bildübertragung in Echtzeit stelle jedenfalls eine Verarbeitung im Sinne des Art. 4 Z 2 DSGVO dar und könne nach Art. 6 Abs. 1 lit. f DSGVO rechtmäßig sein, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen.

Das Bundesverwaltungsgericht führte neuere Rechtsprechung des OGH zum „höchstpersönlichen Lebensbereich“ an, wonach es einer Wertung, bei welcher dem Interesse am gefährdeten Gut stets auch die Interessen der Handelnden und die der Allgemeinheit gegenübergestellt werden müssen (vgl. OGH 27. 06. 2019, 6 0b 6/19d), bedürfe.

In der sodann durchgeführten Interessenabwägung kam das Bundesverwaltungsgericht zum Schluss, dass sich die vorliegende Datenverarbeitung im Lichte der DSGVO als gerechtfertigt darstelle, da gemäß Art. 6 Abs. 1 lit. f DSGVO, die Verarbeitung zur Wahrung der berechtigten Interessen (nämlich des Schutzzwecks) des Verantwortlichen erforderlich ist und diese die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Das Bundesverwaltungsgericht begründete dieses Ergebnis damit, dass die Installation eines (mechanischen bzw. digitalen) Türspions grundsätzlich ein geeignetes Mittel darstelle, um potentielle Gefahren vor Öffnen der Türe zu erkennen, wobei ein gelinderes Mittel zu diesem Zweck nicht zur Verfügung stehe. Es handle es sich beim Einsatz des digitalen Türspions zwar um eine Echtzeitüberwachung, die Gefährdung schutzwürdiger Geheimhaltungsinteressen sei bei derartigen Systemen - ohne Speicherung und Aufnahme von Bilddateien - jedoch deutlich herabgesetzt. Dazu komme, dass der verfahrensgegenständliche digitale Türspion nur bei Knopfdruck eine zehnstündige Aufnahme in Echtzeit übertrage und weder über eine Auf-

zeichnungsfunktion verfüge, noch eine Speicherung vornehme, weshalb von einer vom OGH in seiner Entscheidung angesprochenen fortdauernden unerwünschten Überwachung nicht die Rede sein könne.

Die Entscheidung ist rechtskräftig.

3.2.6a Beschwerdeverfahren vor dem Bundesverwaltungsgericht in Verwaltungsstraftsa- chen

Seit dem in Geltung treten der Datenschutz-Grundverordnung wurden 11 Beschwerden gegen Straferkenntnisse der Datenschutzbehörde erhoben.

Erkenntnis des Bundesverwaltungsgerichtes vom 19.08.2019, GZ W211 2208885-1/19E

Das Bundesverwaltungsgericht hat einer Beschwerde gegen den Bescheid der Datenschutzbehörde vom 12. September 2018, GZ DSB D550.038/0003-DSB/2018, Folge gegeben.

Dem mit Erkenntnis des Bundesverwaltungsgerichtes behobenen Straferkenntnis der Datenschutzbehörde ging voraus, dass zu einem näher bestimmten Tatzeitpunkt durch zwei Beamte einer Polizeiinspektion am Standort eines Sportwetten-Cafés eine Kontrolle nach dem Glücksspielgesetz durchgeführt worden war. Bei dieser Kontrolle stellten die Beamten zwei sichtbar montierte Kameras sowie im Geschäftslokal Bildschirme fest. In Hinblick auf diese Wahrnehmungen sowie die Angaben einer Kellnerin im Geschäftslokal, wurde eine Anzeige wegen Verdachts auf den Betrieb meldepflichtiger Videoüberwachungskameras und Nichtkennzeichnung einer solchen Anlage erstattet. Die Datenschutzbehörde forderte die beschuldigte juristische Person zu Handen ihres Geschäftsführers im Zuge des Ermittlungsverfahrens zur Rechtfertigung auf und gab darin bekannt, dass ein Verdacht im Hinblick auf die in § 62 Abs. 3 iVm § 30 Datenschutzgesetz – DSG, in der Fassung BGBl. I Nr. 24/2018, und Art. 83 DSGVO vorgesehene Möglichkeit der Verhängung einer Geldstrafe gegen die beschuldigte juristische Person bestünde. Seitens der beschuldigten juristischen Person wurde jedoch keine Stellungnahme im Ermittlungsverfahren abgegeben.

Daraufhin erließ die Datenschutzbehörde das mit dem gegenständlichen Erkenntnis des Bundesverwaltungsgerichtes aufgehobene Straferkenntnis und sprach aus, dass die beschuldigte juristische Person (zumindest ab einem näher bestimmten Zeitpunkt) am Standort des Geschäftslokals als Verantwortliche im Sinne des Art. 4 Z 7 DSGVO eine Bildverarbeitungsanlage (Videoüberwachung) betreibe und – bezogen auf den zeitlichen Anwendungsbereich der DSGVO – dadurch u. a. Art. 5 Abs. 1 lit. a und lit. c und Art. 6 Abs. 1 DSGVO verletzt habe. Gestützt wurde die Verhängung der Geldstrafe zumindest teilweise auf Art. 83 Abs. 5 DSGVO.

Das Bundesverwaltungsgericht hob das Straferkenntnis mit der Begründung auf, dass es die Datenschutzbehörde unterlassen habe, den (vorgeworfenen) Verstoß einer konkreten natürlichen Person im Sinne des § 30 Abs. 1 und Abs. 2 DSG vorzuwerfen, welche für die juristische Person gehandelt habe. Dies alles unter Verweis auf das Erkenntnis des Verwaltungsgerichtshofes vom 29. März 2019, Ro 2018/02/0023, in dem sich der Verwaltungsgerichtshof mit der Strafbarkeit juristischer Personen im Sinne des 99d BWG bzw. des § 35 FM-GwG auseinandergesetzt hatte.

Gegen das Erkenntnis des Bundesverwaltungsgerichtes erhob die Datenschutzbehörde eine Amtsrevision und führte darin mit Blick auf die Zulässigkeitsgründe derselben aus, dass die grundsätzliche Rechtsfrage u. a. darin gelegen sei, ob für die wortgemäße Anwendung des § 30 Abs. 1 und Abs. 2 DSG im Anwendungsbereich von Art. 83 DSGVO überhaupt ein Raum verbleibt, wenn § 30 DSG die Verhängung von Geldbußen gegen juristische Personen als Ver-

antwortliche iSd Art 4 Z 7 DSGVO an das Vorliegen von zu Art. 83 DSGVO hinzutretenden (nationalrechtlichen) Tatbestandsvoraussetzungen knüpft, wodurch eine unionsweite einheitliche Auslegung und Anwendung von Art. 83 DSGVO erheblich beeinträchtigt erscheint.

Das Verfahren über die ordentliche Revision war zu Redaktionsschluss des Berichts beim Verwaltungsgerichtshof anhängig.

Erkenntnis des Bundesverwaltungsgerichtes vom 25. November 2019, GZ W211 2208885-1/19E

Das Bundesverwaltungsgericht hat einer Beschwerde gegen das Straferkenntnis der Datenschutzbehörde vom 18. Oktober 2018, DSB-D550.048/0004-DSB/2018, teilweise Folge gegeben.

Dem mit Erkenntnis des Bundesverwaltungsgerichts behobenen Straferkenntnis der Datenschutzbehörde liegt – soweit hier wesentlich – der folgende Sachverhalt zu Grunde: Basierend auf den Erhebungen eines Sicherheitswachebeamten übermittelte die örtlich zuständige Bezirksverwaltungsbehörde eine Sachverhaltsdarstellung an die Datenschutzbehörde, die zum Gegenstand hatte, dass bei einem Kebab Stand drei Videokameras betrieben werden, wobei zwei davon im Innenraum und eine der Kameras an einem Lagercontainer installiert seien. In dem Container befinde sich auch ein PC, auf dem die Bilder der Kameras in Echtzeit angezeigt und nach Angaben des Beschuldigten bis zu 16 Tage gespeichert würden. Die Außenkamera filme bis zu einer Waschanlage einer Tankstelle, während die anderen beiden Kameras den Innenbereich der Durchreiche ins Vorzelt und den Arbeitsbereich abdecken würden. Hinweisschilder auf die Videoüberwachung seien weder innen noch außen angebracht. Zur Installation und zum Zweck der Videoüberwachung gab der Beschuldigte an, dass er diese selbst gekauft und installiert habe, um die (seiner Ansicht nach rechtswidrigen) Amtshandlungen eines namentlich genannten Polizisten zu dokumentieren.

Die Datenschutzbehörde richtete daraufhin eine Aufforderung zur Rechtfertigung an den Beschuldigten als Verantwortlichen iSv Art. 4 Z 7 DSGVO und warf diesem darin vor, dass die zulässige Speicherdauer von 72 Stunden überschritten werde, die Videoüberwachung nicht (geeignet) gekennzeichnet werde und eine öffentliche Straße miterfasse – somit nicht auf Bereiche beschränkt sei, welche in der ausschließlichen Verfügungsbefugnis des Verantwortlichen stehen würden; diese daher nicht dem Zweck angemessen und nicht auf das notwendige Maß beschränkt sei, wodurch der Verdacht der Verletzung des § 13 Abs. 3 und Abs. 5 DSG und der Art. 5 Abs. 1 lit. a und lit. b sowie Art. 6 Abs. 1 DSGVO bestünde. Daraufhin gab der Beschwerdeführer im Rahmen seiner Rechtfertigung zum Tatvorwurf an, dass die Videoüberwachung stets durch sehr gut wahrnehmbare Hinweisschilder [...] gekennzeichnet gewesen sei und die zulässige Speicherdauer lediglich auf Grund eines Rechtsirrtums überschritten worden sei. Unrichtig sei weiter, dass die Videoüberwachung eine öffentliche Straße und eine Tankstelle erfasst hätte. Das einzige, was überwacht werde, sei jener Bereich, welcher in der ausschließlichen Verfügungsbefugnis der Gewerbeinhaberin stehe [...].

Daraufhin erließ die Datenschutzbehörde das angefochtene Straferkenntnis und legte dem Beschwerdeführer darin Verstöße gegen die Art. 5 Abs. 1 lit. a und c sowie Art. 6 Abs. 1 DSGVO zur Last, da die gegenständliche Videoüberwachung auch eine öffentliche Straße erfasste und daher dem Zweck der Verarbeitung nicht angemessen und nicht auf das notwendige Maß beschränkt sei. Zudem bezog sich die verhängte Geldbuße auf den Verstoß gegen § 13 Abs. 3 und Abs. 5 DSG, da Bilddaten bis zu 14 Tage gespeichert worden seien und die Videoüberwachung nicht geeignet gekennzeichnet sei. Die Geldbuße wurde dabei mit insgesamt € 1.800,00 bzw. mit fünf Tagen Ersatzfreiheitsstrafe festgelegt.

Das Beschwerdevorbringen im Hinblick auf das Vorhandensein einer geeigneten Kennzeichnung der Videoüberwachungsanlage verwarf das Bundesverwaltungsgericht unter Hinweis auf im Akt befindliche Lichtbilder, auf denen die vom Beschwerdeführer ins Treffen geführten Hinweisschilder nicht ersichtlich seien.

Das Bundesverwaltungsgericht bestätigte auch die Rechtsansicht der Datenschutzbehörde, dass im vorliegenden Fall das grundrechtlich geschützte Recht auf Geheimhaltung der zufällig im Aufnahmebereich vorbeikommenden VerkehrsteilnehmerInnen ein allfälliges berechtigtes Interesse iSd Art. 6 Abs. 1 lit. f DSGVO am Betrieb der Videoüberwachung (mit dem erweiterten Erfassungsbereich) überwiegt. Einen - darüber hinausgehenden - Tatbestand für die Rechtmäßigkeit des erweiterten Erfassungsbereichs der Kamera am Lagercontainer (vgl. Art. 6 Abs. 1 lit. a. — e. DSGVO) brachte der Beschwerdeführer nicht vor und ergebe sich ein solcher auch nicht aus dem Verfahren. Damit sei der objektive Tatbestand einer Verletzung des Art. 5 Abs. 1 lit. c und des Art. 6 Abs. 1 lit. f DSGVO erfüllt, da weder dem Grundsatz der Datenminimierung gefolgt wurde, noch ein ausreichendes berechtigtes Interesse des Beschwerdeführers gegeben gewesen sei.

Betreffend §§ 12, 13 DSG ging das Bundesverwaltungsgericht jedoch (unter Verweis auf das deutsche Bundesverwaltungsgericht in einer Entscheidung vom 27.03.2019, BVwerg 6 C 2.18 und EuGH, 09.03.1977, C-106/77) davon aus, dass für die Anwendung des § 13 DSG mangels entsprechender Öffnungsklausel in der DSGVO kein Raum bestehe und dieser daher unangewendet zu bleiben habe. Der festgestellte Sachverhalt sei daher ausschließlich unter die entsprechenden Vorschriften der DSGVO zu subsumieren gewesen: Die Aufbewahrung der gespeicherten Bilddaten für einen Zeitraum von 14 Tagen verstieß damit gegen den Grundsatz des Art. 5 Abs. 1 lit. e DSGVO, da sich im Verfahren keinerlei Hinweise darauf ergeben haben, dass mit der Speicherung der Daten für 14 Tage tatsächlich ein unbedingt erforderliches Mindestmaß eingehalten wurde. Selbst wenn von einer Notwendigkeit der Videoüberwachung für Versicherungszwecke ausgegangen werden soll, kann sich eine derart lange Speicherung aus der Notwendigkeit der Nachvollziehbarkeit eines versicherungsrelevanten Vorfalls nicht ergeben. Damit sei dieser Speicherdauer auch jede Grundlage im Rahmen einer Verhältnismäßigkeitsprüfung des Art. 6 Abs. 1 lit. f DSGVO entzogen, da ein derart berechtigtes Interesse des Beschwerdeführers weder vorgebracht worden sei, noch sich aus dem angegebenen Zweck für den Betrieb der Videoanlage ergebe. Daher sei die lange Aufbewahrungsdauer der Bilddaten ebenfalls als ein Verstoß gegen Art. 5 Abs. 1 lit. e und Art. 6 Abs. 1 lit. f DSGVO zu werten und in weiterer Folge unter die Sanktionsnorm des Art. 83 Abs. 1 und Abs. 5 lit. a DSGVO zu subsumieren gewesen.

In Bezug auf die fehlende Kennzeichnung der Videoüberwachungsanlage verweist der erkennende Senat auf die oben ausgeführte Erklärung dazu, dass die Rechtsgrundlage des § 13 Abs. 5 DSG unangewendet zu bleiben habe, und der festgestellte Sachverhalt unter die entsprechenden Vorschriften der DSGVO zu subsumieren sei: Demnach nahm der Beschwerdeführer keine Kennzeichnung seiner Videoüberwachung vor und verstieß damit gegen das Transparenzgebot des Art. 5 Abs. 1 lit. a iVm Art. 12 und Art. 13 DSGVO. Die Strafbarkeit dieses Verstoßes gründe sich ebenso auf Art. 83 Abs. 1 und 5 DSGVO.

Da laut den vom Bundesverwaltungsgericht getroffenen Feststellungen in Bezug auf die Speicherdauer und die Kennzeichnung durch den Beschwerdeführer anlässlich des Verfahrens vor der DSB ein rechtmäßiger Zustand durch den Beschwerdeführer hergestellt wurde, war der Beschwerde hinsichtlich des Ausspruches über die verhängte Strafe teilweise Folge zu geben und ist die verhängte Geldbuße daher mit dem gegenständlichen Erkenntnis auf EUR 1.500,- reduziert worden.

Erkenntnis vom 16.10.2019, GZ: W256 2222862-1/4E

Das Bundesverwaltungsgericht hat einer Beschwerde gegen den Bescheid der Datenschutzbehörde vom 28. Juni 2019, GZ DSB D550.144, Folge gegeben und das Straferkenntnis ersatzlos behoben.

Mit dem durch das Bundesverwaltungsgericht behobenen Straferkenntnis der Datenschutzbehörde verhängte die belangte Behörde eine Geldbuße gegen den Lenker eines KFZ wegen des Betriebs zweier Dash-Cams jedenfalls zu einem näher bestimmten Zeitpunkt, jedoch implizit auch wegen des Betriebs der Dash-Cams auf Fahrten vor dem im Spruch genannten Zeitpunkt. Die belangte Behörde begründete dies in rechtlicher Hinsicht dahingehend, dass die verfahrensgegenständliche Dash-Cam nicht dem Zweck angemessen und nicht auf das notwendige Maß beschränkt war, da andere Verkehrsteilnehmer „insbesondere dann, wenn kein Unfallgeschehen vorliegt, vernünftigerweise nicht damit rechnen müssen, aufgenommen zu werden“, weshalb die verfahrensgegenständliche Dash-Cam gegen die in Art. 5 DSGVO normierten Grundsätze verstoße. Näher hin begründete die DSB diese Entscheidung damit, dass die verfahrensgegenständliche Dash-Cam Bilddaten nicht bloß dann aufzeichnete, wenn es zu einem Unfall komme, sondern bereits mehrere Minuten davor Bilddaten gespeichert werden und zudem der Überschreibungsprozess durch ein bloßes Ziehen der Speicherkarte (jederzeit) unterbrochen werden könne.

Das Bundesverwaltungsgericht folgte der Rechtsansicht der belangten Behörde nicht und führte aus, dass die Behörde unzutreffender Weise jedenfalls von einem überwiegenden Interesse der Verkehrsteilnehmer an der Nichtverarbeitung ihrer Daten gegenüber einem Interesse des Verantwortlichen an der Verarbeitung dieser Daten ausgegangen sei sowie weiters, dass es dem Bundesverwaltungsgericht aufgrund des eingegrenzten Tatzeitpunktes verwehrt sei, in der Sache selbst zu entscheiden und damit nur mit einer Aufhebung des angefochtenen Bescheides vorzugehen gewesen sei; die ordentliche Revision wurde für zulässig erklärt.

Die Datenschutzbehörde erhob gegen das Erkenntnis des Bundesverwaltungsgerichtes Amtsrevision.

Das Verfahren über die ordentliche Revision ist derzeit beim Verwaltungsgerichtshof anhängig.

3.2.7 Verfahren über die Meldung der Verletzung des Schutzes personenbezogener Daten

92 inländische, 11 grenzüberschreitende sowie 71 Sicherheitsverletzungen („Data Breach“), die bei ausländischen Aufsichtsbehörden eingelangt sind, wurden der Datenschutzbehörde im Berichtszeitraum gemeldet. Darüber hinaus haben Betreiber öffentlicher Kommunikationsdienste 44 Meldungen gem. § 95a TKG 2003 erstattet.

Bei den gemeldeten Sicherheitsverletzungen handelte es sich häufig um Fälle menschlichen Versagens („Versenden von E-Mails an einen falschen Adressaten“, „Versenden von E-Mails im offenen statt im geschlossenen Verteiler“ etc.), verlorener oder gestohlener Geräte (insbesondere Notebooks und Handys) oder um sog. „Ransomware“ (Verschlüsselung von Daten durch Schadsoftware).

Folgender Fall sei exemplarisch für die zweite Fallgruppe angeführt:

Im Zusammenhang mit einem unbeaufsichtigten Sack mit Briefen vor einem Bürogebäude wurde aufgrund der Anregung einer Einschreiterin ein amtswegiges Prüfverfahren gegen die Ver-

antwortliche eingeleitet. In dem Sack befanden sich die gesammelten Briefsendungen der Einschreiterin sowie weitere Briefe für den Zustellbereich des Mitarbeiters der Verantwortlichen.

Die Verantwortliche hatte diesbezüglich keine Meldung iSd Art. 33 DSVO erstattet.

Entgegen der Ansicht der Verantwortlichen, die DSGVO sei nicht anwendbar, führte die Datenschutzbehörde im Bescheid vom 13. August 2019 mit der GZ: DSB-D205.213/0002-DSB/2019 aus, dass dies nicht zutrifft, weil insbesondere der in Art. 4 Z 6 DSGVO legaldefinierte Begriff des „Dateisystems“ erfüllt ist, da die Verantwortliche schon in der Distribution offensichtlich automatisierte, teilautomatisierte und anhand eines Systems manuelle Schritte der Zuordnung von Daten (Postbriefen) setzt und diese an verschiedene Zusteller verteilt – die Zuordnung erfolgt anhand der Postleitzahl und der Zustelladresse –, die in ihrem Zustellungsbereich die weitere Zuordnung vornehmen sollen.

Festgestellt wurde neben einer Verletzung der Meldepflicht des Art. 33 DSGVO eine Verletzung der Pflicht der Verantwortlichen, die Integrität und Vertraulichkeit der Datenverarbeitung sowie die erforderlichen Sicherheitsmaßnahmen zu gewährleisten. Begründend hat die Datenschutzbehörde ausgeführt, dass weder, wie die Verantwortliche repliziert hatte, das generelle Hemmnis, Straftaten zu begehen, noch ein loses Band, mit dem der Postsack zugeschnürt war oder die Aufschrift mit dem Eigentumshinweis der Verantwortlichen hinreichende technische und organisatorische Maßnahmen iSd Art 5 Abs.1 lit. f und Abs. 2 iVm Art. 32 DSGVO darstellen.

Aufgrund des Bescheides im amtswegigen Prüfverfahren wurde ein (abgekürztes) Verwaltungsstrafverfahren gegen die Verantwortliche eingeleitet, welches in einer Strafverfügung mündete, mit der eine Geldstrafe iHv. EUR 600,- verhängt wurde, welche die Verantwortliche mittels Einspruch bekämpfte. Das Verfahren ist anhängig.

3.2.8 Konsultationsverfahren

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche gemäß Art. 35 DSGVO vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Geht aus dieser Datenschutz-Folgenabschätzung hervor, dass, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, die beabsichtigte Verarbeitung ein hohes Risiko zur Folge hätte, hat der Verantwortliche die Aufsichtsbehörde zu konsultieren. Im Rahmen dieses Konsultationsverfahrens gemäß Art. 36 DSGVO hat die Aufsichtsbehörde verschiedene Befugnisse. Einerseits kann sie dem Verantwortlichen bzw. dem Auftragsverarbeiter schriftliche Empfehlungen unterbreiten, sofern sie der Ansicht ist, dass die geplante Verarbeitung nicht im Einklang mit der DSGVO steht, etwa, weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat. Darüber hinaus kann die Aufsichtsbehörde sämtliche in Art. 58 DSGVO genannten Befugnisse ausüben.

Im Jahr 2019 wurde die Datenschutzbehörde als Aufsichtsbehörde in insgesamt vier Fällen gemäß Art. 36 DSGVO konsultiert. Zwei Anträge wurden in weiterer Folge zurückgezogen und das Verfahren eingestellt, da schon aus der übermittelten Datenschutz-Folgenabschätzung jeweils hervorging, dass die beabsichtigte Datenverarbeitung bei Anwendung der ausgearbeiteten Abhilfemaßnahmen kein hohes Risiko zur Folge hätte. In einem Verfahren wurde die Datenschutzbehörde von einem Unternehmen konsultiert, welches sich auf Identitätsprüfung spezialisiert hat. Unternehmen, die im Zuge einer Geschäftsanbahnung Ausweise von potenziellen Kunden erhalten haben, können diese bei dem Unternehmen auf Echtheit überprüfen lassen. Bislang

hat das Unternehmen die Überprüfung nur isoliert von Ausweisen anderer Kunden durchgeführt. Nun soll jedoch eine Datenbank gefälschter Ausweise erstellt werden, sodass im Zuge der Überprüfung eines Ausweises auch ein Abgleich mit bereits als gefälscht identifizierten Ausweisen möglich sein soll. Aus der übermittelten Datenschutz-Folgenabschätzung geht hervor, dass die beabsichtigte Datenverarbeitung ein hohes Risiko zur Folge hätte. Das Verfahren ist zum Zeitpunkt des Redaktionsschlusses anhängig.

3.2.9 Anträge auf Genehmigung von Verhaltensregeln

Bis Ende Februar 2020 wurden seit Geltung der DSGVO insgesamt zehn Anträge auf Genehmigung von Verhaltensregeln an die Datenschutzbehörde gestellt, wovon sieben Verhaltensregeln unter der aufschiebenden Bedingung genehmigt wurden, dass in Folge eine entsprechend dazugehörige Überwachungsstelle gemäß Art. 41 Abs. 2 DSGVO akkreditiert wird. Da eine endgültige Genehmigung noch aussteht, wurden die Verhaltensregeln seitens der Datenschutzbehörde noch nicht veröffentlicht. Sobald dies der Fall ist, wird die Datenschutzbehörde auf ihrer Webpage ein entsprechendes öffentliches Verzeichnis für genehmigte Verhaltensregeln gemäß Art. 40 Abs. 6 DSGVO führen.

Zu den bisher (unter aufschiebender Bedingung) genehmigten Verhaltensregeln zählen:

- Verhaltensregeln für Internet Service Provider⁶
- Verhaltensregeln für die Ausübung des Gewerbes der Adressverlage und Direktmarketingunternehmen gem. § 151 Gewerbeordnung 1994⁷
- Verhaltensregeln für Garagen- und Parkplatzbetriebe⁸
- Verhaltensregeln für Netzbetreiber bei der Verarbeitung von mit intelligenten Messgeräten erhobenen personenbezogenen Daten von Endverbrauchern nach den §§ 83 ff. ElWOG 2010⁹
- Verhaltensregeln für Presse- und Magazin-Medienunternehmen (teils nicht rechtskräftig)
- Verhaltensregeln für Bilanzbuchhaltungsberufe (Bilanzbuchhalter, Buchhalter, Personalverrechner)¹⁰
- Verhaltensregeln zum Datenschutz der Berufsvereinigung der ArbeitgeberInnen privater Bildungseinrichtungen (BABE)¹¹

Ausgehend von den bisherigen Anträgen zeichnet sich ab, dass der Frage der datenschutzrechtlichen Rollenverteilung (unter Berücksichtigung datenschutzrechtlicher Materiegesetze), den Modalitäten und der Ausübung von Betroffenenrechten nach Kapitel III DSGVO, der Umsetzung der Informationspflichten nach Art. 13 bzw. Art. 14 DSGVO sowie der Einhaltung der in der DSGVO verankerten Rechenschaftspflichten besondere Aufmerksamkeit gewidmet wird. Die nähere Regelung von technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO spielte bislang eine untergeordnete Rolle, die Übermittlung von per-

6 Veröffentlicht durch den Antragsteller unter <https://www.ispa.at/wissenspool/datenschutz.html> (nicht authentische Fassung).

7 Veröffentlicht durch den Antragsteller unter <https://www.dmvoe.at/2019/06/14/verhaltensregeln-dialog-marketing> (nicht authentische Fassung).

8 Veröffentlicht durch den Antragsteller unter <https://www.wko.at/branchen/transport-verkehr/garagen-tankstellen-serviceunternehmungen/verhaltensregeln-garagenunternehmungen.html> (nicht authentische Fassung).

9 Veröffentlicht durch den Antragsteller unter <https://oesterreichsenergie.at/die-welt-des-stroms/stromnetze/smart-meter/verhaltensregeln-smart-meter.html> (nicht authentische Fassung).

10 Veröffentlicht durch den Antragsteller unter <https://www.wko.at/branchen/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/buchhaltung/verhaltensregeln-bilanzbuchhaltungsberufe-dsgvo.html> (nicht authentische Fassung).

11 Veröffentlicht durch den Antragsteller unter <http://www.babe.or.at/1027,1103,0,2.html> (nicht authentische Fassung).

sonenbezogenen Daten an Drittländer oder an internationale Organisationen nach Art. 46 Abs. 2 lit. e DSGVO war noch nicht Gegenstand von Verhaltensregeln.

Weiterführende Informationen zu diesem Thema sind in den Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679 des Europäischen Datenschutzausschusses¹² sowie im Informationsblatt der Datenschutzbehörde¹³ zu finden.

3.2.10 Die Verhängung von Geldbußen durch die Österreichische Datenschutzbehörde

Seit in Geltung treten der Europäischen Datenschutz-Grundverordnung (im Folgenden kurz: DSGVO) am 25. Mai 2018 kommt der Österreichischen Datenschutzbehörde (DSB) als nationaler Aufsichtsbehörde gemäß Art. 58 Abs. 2 lit. i DSGVO die Aufgabe zu, Geldbußen wegen Verstößen gegen die bußgeldbewehrten Bestimmungen im Sinne deren Art. 83 zu verhängen.

In diesem Zusammenhang hat die DSB bislang 38 Geldbußen und 11 Verwarnungen (Art 58 Abs. 2 lit. b) ausgesprochen. Insgesamt hat die DSB Geldbußen im Gesamtausmaß von € 18.106.700,00 verhängt.

Zu den bisher verfolgten Rechtsverletzungen

Bildverarbeitung

Insbesondere in Fällen von Verfahren gegen Privatpersonen bildete der (unrechtmäßige) Betrieb von Bildverarbeitungsanlagen, wie etwa Videoüberwachungseinrichtungen in und außerhalb von privaten Gebäuden sowie in Fahrzeugen installierte Kamerasysteme (sog. Dash-Cams), den Gegenstand von Verfahren zur Verhängung von Geldbußen gemäß Art. 83 DSGVO.

Immer wieder zeigte sich dabei, dass vielen Verantwortlichen nicht bewusst ist, dass durch den Einsatz von Videoüberwachungsanlagen, etwa zur Überwachung des Außenbereiches ihres Wohnhauses oder ihrer Wohnung, wenn diese auch Teile des umliegenden öffentlichen Raumes wie Gehsteige und Straßenteile miterfassen, in die Rechte von unbeteiligten Personen eingegriffen werden kann und ein solcher Eingriff sowohl gegen die Datenverarbeitungsgrundsätze des Art. 5 Abs. 1 DSGVO als auch gegen die von Art. 6 Abs. 1 DSGVO normierten abschließend aufgezählten Rechtmäßigkeitstatbestände der DSGVO verstoßen können.

Darüber hinaus wurden in mehreren Fällen Geldbußen gegen Verantwortliche verhängt, die in ihrem Auto eine Dash-Cam betrieben haben und über längere Zeiträume hindurch den öffentlichen Straßenverkehr – und damit auch andere Straßenverkehrsteilnehmer – aufgezeichnet haben.

Die DSB verhängte am 11.07.2019 in einem besonders schwerwiegenden Fall gegen einen Fußballtrainer einer Frauenfußballmannschaft eine Geldbuße von € 10.000, GZ: DSB-D550.185/0002 -DSB/2019, weil dieser zwei Fußballspielerinnen heimlich in der Damenumkleidekabine des Fußballvereins gefilmt hatte, während diese sich zum Umkleiden und Duschen nackt darin aufgehalten haben.

Zur datenschutzrechtlichen Qualifikation von Bildverarbeitungsvorgängen sei an dieser Stelle auf ein rezentes Urteil des Europäischen Gerichtshofes vom 11.12.2019 hingewiesen¹⁴.

12 https://www.dsb.gv.at/europaischer_datenschutzausschuss_edsa

13 <https://www.dsb.gv.at/genehmigung-von-verhaltensregeln>

14 Vgl. Urteil des EuGH vom 11.12.2019, C-708/18, Rz 37ff; siehe nähere Darstellung im Kapitel 4.5.

Die dort aufgezählten Punkte können als „Leitlinie“ zur Beurteilung jeglicher Form der Bildverarbeitung (stationär, mobil, Dashcam) herangezogen werden. In jedem Fall wird jedoch eine Einzelfallbeurteilung geboten sein, in der die Interessen des Verantwortlichen und die berechtigten Interessen betroffener Personen und deren Erwartungshaltung sorgfältig abzuwägen sein werden.

Direktmarketing und Data Broking

Die DSB hat am 23.10.2019, GZ: DSB-D550.148/0017-DSB/2019, eine Geldbuße gegen die Österreichische Post AG in der Höhe von € 18.000.000,00 verhängt, da diese im Rahmen deren gewerblicher Tätigkeit als Adressverlag und Direktmarketingunternehmen unter anderem Daten zur politischen Affinität einzelner identifizierter Personen erstellt und an politische Parteien vermarktet hat. Dies indem durch statistische Verfahren einzelnen Personen in einer Adressdatenbank vermeintliche politische Präferenzen zugeordnet und diese Informationen sodann vermarktet wurden. Zudem wurde festgestellt, dass die Österreichische Post AG Daten zur Umzugshäufigkeit und zur Anzahl empfangener Pakete einzelner Kunden, die sie zunächst im Rahmen ihrer Tätigkeit als Postdienstleister nach dem Postmarktgesetz notwendigerweise erfasst hat, im Rahmen ihres Geschäftszweiges Adressverlag und Direktmarketing an andere Unternehmen weitervermarktet hat.

Die wegen der festgestellten Verstöße gegen die Art. 5 Abs. 1, 6 Abs. 1 und 4 sowie 9 DSGVO verhängte Strafe ist nicht rechtskräftig, da von der Beschuldigten dagegen das Rechtsmittel der Beschwerde an das Bundesverwaltungsgericht eingebracht wurde.

Sonstige Verstöße

In einer weiteren Entscheidung hat die DSB am 12.08.2019, GZ: DSB-D550.095/0002-DSB/2019, gegen den Betreiber eines Ärztezentrums eine Geldbuße in der Höhe von € 50.000,00 verhängt. In diesem Fall hat die datenschutzrechtlich Verantwortliche – es handelt sich um eine Gesellschaft mit beschränkter Haftung – in mehrfacher Hinsicht gegen die Verpflichtungen der DSGVO verstoßen, nämlich unter Anderem

- durch die Nicht-Benennung eines Datenschutzbeauftragten gegen die Pflicht nach Art. 37 Abs. 1 lit. c DSGVO sowie gegen ihre Pflichten gemäß Art. 37 Abs. 7 zur Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten und Mitteilung dieser Daten an die DSB,
- durch die Nichterfüllung der Voraussetzungen für die Einholung einer Einwilligung von Patienten gegen die Bestimmungen des Art 7 DSGVO, indem die Einwilligungserklärung Sachverhalte erfasste, die keiner Einwilligung unterliegen, jedoch den Anschein erweckten, dass hierfür eine Einwilligung zu erteilen war, und der Einwilligungserklärung nicht mit hinreichender Klarheit zu entnehmen war, für welche Datenverarbeitungen die Einwilligung die Rechtsgrundlage sein sollte, sowie
- gegen die Pflicht zur Prüfung der Notwendigkeit einer Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO bezüglich der typischerweise in einer Gesundheitseinrichtung stattfindenden Datenverarbeitungsvorgänge, wie beispielsweise der Verwaltung von medizinischen Befunden und sonstigen Patientendaten.

3.2.11 Stellungnahmen zu Gesetzes- und Verordnungsentwürfen

Die Datenschutzbehörde hat im Jahr 2019 zu folgenden Vorhaben eine Stellungnahme abgegeben. Die Stellungnahmen sind, soweit es sich nicht um jene zu Verordnungen oder Landesgesetzen handelt, unter www.parlament.gv.at abrufbar.

- Stellungnahme zum Entwurf eines Bundesgesetzes, mit dem das Bundesgesetz über den barrierefreien Zugang zu Websites und mobilen Anwendungen des Bundes erlassen wird (Web-Zugänglichkeits-Gesetz – WZG)

- Wehrrechtsänderungsgesetz 2019
- Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung, mit der die Hochschülerinnen- und Hochschülerschaftswahlordnung 2014 – HSWO 2014 geändert wird
- Entwurf Strahlenschutzgesetz 2019
- Novelle Wiener Abfallwirtschaftsgesetz
- Novellierung der Zuteilungsregelverordnung
- Grundbuchs-Novelle 2019
- 2. Dienstrechts-Novelle 2019
- Bundesgesetz, mit dem ein Bundesgesetz über Sorgfalt und Verantwortung im Netz erlassen und das KommAustria-Gesetz geändert wird
- E-Card Foto-Verordnung
- 3. Änderung der Datenschutzverordnung für die Sozialversicherung (SV-DV)
- Novelle des Wr. Gebrauchsabgabengesetzes
- Integrationsgesetz-Durchführungsverordnung
- Strafvollzugsgesetz-Novelle 2019
- Transparenzdatenbank-Abfrageverordnung 2019
- Novelle des WTBG 2017 und des BiBuG 2019 zur Umsetzung der 5. Geldwäsche-Richtlinie
- Novelle der GewO 1994 zur Umsetzung der 5. Geldwäsche-Richtlinie (Geldwäschenovelle 2019)
- Wr. Veranstaltungsgesetz 2020
- Forschungsrahmennovelle (BMVIT) 2019

4 Wesentliche höchstgerichtliche Entscheidungen

4.1 Verfahren vor dem Verfassungsgerichtshof

Im Berichtszeitraum sind folgende datenschutzrechtlich relevante Entscheidungen des Verfassungsgerichtshofes ergangen:

1. Beschluss vom 25.2.2019, E 4577/2018

(Klaglosstellung vor dem VfGH durch Zurückziehung eines Antrags auf Auskunft)

In diesem Einstellungsbeschluss hat der Verfassungsgerichtshof festgehalten, dass ein Beschwerdeführer (vor der Datenschutzbehörde: Beschwerdegegner, es handelte sich um einen Verantwortlichen, dem von der Datenschutzbehörde eine Auskunftserteilung aufgetragen worden war) im Verfahren vor dem Höchstgericht als klaglos gestellt gilt, wenn die mitbeteiligte Partei (Vor der Datenschutzbehörde: Beschwerdeführer) den ursprünglichen Antrag auf Auskunftserteilung zurückgezogen hat. Die Tatsache, dass ein den Bescheid der Datenschutzbehörde bestätigendes Erkenntnis des Bundesverwaltungsgerichts damit endgültig formell in Rechtskraft erwächst, schadet der Klaglosstellung nicht, da die erfolgte Zurückziehung erfolgreich einem Vollstreckungsantrag entgegengehalten werden könnte.

2. Beschluss vom 14.6.2019, G 385/2018

(Individualantrag auf Gesetzesprüfung, Zumutbarkeit des datenschutzrechtlichen Beschwerdewegs)

In diesem Beschluss hat der Verfassungsgerichtshof einen Individualantrag gemäß Art. 140 Abs. 1 Z 1 lit c des Bundes-Verfassungsgesetzes auf Aufhebung von Bestimmungen des GesundheitstelematikG 2012 betreffend ELGA-Gesundheitsdaten unter anderem wegen der Zumutbarkeit der Erwirkung eines Bescheids der Datenschutzbehörde (im Beschwerdeverfahren gemäß § 24 DSG) zurückgewiesen.

3. Erkenntnis vom 10.10.2019, E 1025/2018

(Verpflichtung eines Verwaltungsgerichts, über Beschwerde einer Partei wegen Geheimhaltungsverletzungen der Verwaltungsbehörde zu entscheiden)

Dieses Erkenntnis befasst sich in seinen Erwägungen zwar hauptsächlich mit Fragen des (verwaltungsgerichtlichen) Verfahrensrechts, insbesondere der Auslegung der §§ 17 und 45 AVG. Nach Auslegung des Höchstgerichts muss ein Verwaltungsgericht über eine Beschwerde einer durch den ergangenen Bescheid nicht beschwerten Partei entscheiden – die Beschwerde wurde vom Bundesverwaltungsgerichts zurückgewiesen -, wenn diese eine Verletzung im Verfahrensrecht auf Geheimhaltung (Verletzung von Betriebs- und Geschäftsgeheimnissen, geltend gemacht wurde aber auch das Recht auf Geheimhaltung gemäß § 1 DSG) durch die Verwaltungsbehörde behauptet. Anders als im zuletzt zitierten Beschluss war die Frage der Zumutbarkeit der Erwirkung eines Bescheids der Datenschutzbehörde (im Beschwerdeverfahren gemäß § 24 DSG) hier kein Gegenstand der Erwägungen des Verfassungsgerichtshofs.

4. Erkenntnis vom 11.12.2019, G 72/2019 ua

(Verfassungswidrigkeit von Section-Control-Datenauswertung für Sicherheitszwecke und Bundestrojaner)

In diesem Gesetzesprüfungsverfahren auf Antrag eines Drittels der Mitglieder des Nationalrats, hat der Verfassungsgerichtshof wesentliche Bestimmungen des sogenannten „Sicherheitspakets“ (BGBl. I Nr. 29/2018) als verfassungswidrig aufgehoben. Festgestellt wurden eine Verletzung im Recht auf Datenschutz und Achtung des Privatlebens betreffend die Verarbeitung, Übermittlung und – anlasslose – Speicherung von Daten aus Section-Control-Anlagen bzw. verdeckte Erfassung und Speicherung von (Bild-) Daten zur Identifizierung von Fahrzeugen und Fahrzeugkern mittels bildverarbeitender technischer Einrichtungen, eine Verletzung im Recht auf Achtung des Privatlebens durch die Befugnis zur verdeckten Überwachung der Nutzung von Computersystemen und verschlüsselter Nachrichten durch Installation eines Programms („Bundestrojaner“), eine Verletzung im Recht auf Achtung der Privatsphäre betreffend die Überwachung verschlüsselter Nachrichten mangels begleitender, effektiver und unabhängiger Aufsicht über die laufende Durchführung der Maßnahme und eine Verletzung im Hausrechtsgesetz betreffend die Installation eines „Bundestrojaners“ mangels nachträglicher Mitteilungspflicht. Die gesetzlich vorgesehenen Eingriffe wurden mehrfach für unverhältnismäßig befunden.

5. Erkenntnis vom 12.12.2019, G 164/2019 ua

(Pauschale Ermächtigung zur Datenverarbeitung, Verstoß gegen das Determinierungsgebot) In diesem Gesetzesprüfungsverfahren auf Antrag eines Drittels der Mitglieder des Bundesrats hat der Verfassungsgerichtshof betreffend die Bundes- und Bundesgrundsatzgesetzgebung in Angelegenheiten der Mindestsicherung/Sozialhilfe u.a. § 1 Abs. 1 des Sozialhilfe-Statistikgesetzes, BGBl I Nr. 41/2019 als verfassungswidrig (unzulässiger Eingriff in das Grundrecht auf

Datenschutz gemäß § 1 Abs. 1 DSG) aufgehoben, weil die Anordnung, dass „sämtliche Behörden“ verpflichtet sind, den Ländern „die zu Zwecken der Aufrechterhaltung und Vollziehung des österreichischen Sozialhilfewesens erforderlichen Daten“ elektronisch zur Verfügung zu stellen, gegen das Gebot verstößt, festzulegen, wer konkret zur Datenverarbeitung verpflichtet ist, und welche personenbezogenen Daten von der Übermittlung erfasst sein sollen (Determinierungsgebot).

4.2 Oberster Gerichtshof

4.2.1 Videoaufnahmen einer Amtshandlung zu Zwecken der Beweisaufnahme zulässig, nicht aber deren Veröffentlichung (§§ 16 ABGB, 78 UrhG)

Der Oberste Gerichtshof hat im Rahmen einer Revision vom 27. Juni 2019, zu Zl. 6 Ob 6/2019,¹⁵ gegen das Urteil des OLG Linz entschieden, dass ein Unterlassungsbegehren, Lichtbilder und Bildnisse einer polizeilichen Amtshandlung anzufertigen, abgewiesen, dem Unterlassungsbegehren Lichtbilder, Videoaufzeichnungen oder sonstige Bildnisse zu veröffentlichen, hingegen stattgegeben wurde.

Hintergrund:

Im Rahmen des Vollzuges eines gerichtlichen Auftrages zur Eröffnung eines Konkursverfahrens mit Anschlussexécution gegen einen Einzelunternehmer auf dessen Liegenschaft (zwei Gerichtsvollzieher, mehrere maskierte und nicht maskierte Polizeibeamte, teilweise von der Cobra) im Kontext von „Staatsverweigerern“, wurden Videoaufnahmen am Handy durch die Frau des Einzelunternehmers zu Zwecken der Beweisdokumentation angefertigt. Während der Aufnahmen wurde der Name eines Polizeibeamten hörbar erwähnt. In Folge wurde das Video auf youtube allgemein zugänglich eingestellt. Durch wen dies erfolgte, konnte nicht mehr festgestellt werden.

Datenschutzrechtliche Anspruchsgrundlagen wurden nicht geltend gemacht. Ebenso wenig Thema waren Fragen der freien Meinungsäußerung, da – wie erwähnt – von den Beteiligten der youtube upload bestritten wurde.

Begründung:

Zum Anfertigen der Filmaufnahmen hielt der OGH fest:

„Die Staatsgewalt muss bei einem hoheitlichen Einsatz mit Zwangsgewalt akzeptieren, dass diese Vorgänge festgehalten werden, zumal dadurch auch ein gewisser präventiver Effekt gegen allfällige rechtswidrige Übergriffe erreicht wird. Demgegenüber war in der Vorentscheidung der klagende Rechtsanwalt gerade nicht mit der Befugnis zur Ausübung von Zwangsmitteln ausgestattet. Entgegen der Auffassung des Berufungsgerichts kann für die Erlaubtheit des Filmens nicht erforderlich sein, dass etwa der Kläger übergriffig geworden wäre oder Sachen beschädigt hätte: Eine Aufnahme, die erst nach einem erfolgten Übergriff oder einer Beschädigung beginnt, kann den Dokumentationszweck nicht erfüllen.“

Zur Veröffentlichung:

„Bei nicht allgemein bekannten Personen des öffentlichen Lebens wird – so wie bei unbekanntem Privatpersonen – die Verletzung durch die Beigabe des Bildes noch verschärft und eine

15 https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JT_20190627_OGH0002_00600B00006_19D0000_000

„**Prangerwirkung**“ erzielt, weil die Person des Angegriffenen damit erst einer breiten Öffentlichkeit auch optisch kenntlich gemacht wird (RS0077767). **Behauptet derjenige, der das Bild verbreitet, seinerseits ein Interesse an diesem Vorgehen, dann müssen die beiderseitigen Interessen gegeneinander abgewogen werden** (RS0078088 [T2]). Auf die Frage, ob der Veröffentlichender, insbesondere wegen eines nach den Umständen des konkreten Falls gegebenen Informationsbedürfnisses der Öffentlichkeit ein berechtigtes Interesse daran hat, das Bildnis einer Person zu veröffentlichen und zu verbreiten, ist aber regelmäßig nur einzugehen, wenn er darüber entsprechende Behauptungen aufstellt (RS0077785).“

Zur Unterlassungsverpflichtung der Veröffentlichung trotz nicht vorhandenen Beweis, dass es die Beklagte war:

„**Dadurch, dass die Beklagte die Videoaufnahmen angefertigt hat, hat sie im Sinn der unter 2.3.1. zitierten, zum Schadenersatzrecht ergangenen Judikatur eine „verpflichtende Vorhandlung“ gesetzt bzw die Gefahrensituation, dass das Video im Internet veröffentlicht werden könnte, verursacht. Nach dem Ingerenzprinzip ist sie besonders verpflichtet, alles ihr Mögliche vorzukehren, um die Veröffentlichung der Videoaufnahmen des Klägers zu verhindern.** Sie hätte daher zB das Mobiltelefon, mit dem sie die Aufnahmen gemacht hat, nicht aus ihrer Gewahrsame geben dürfen oder es sicher und für andere unzugänglich (versperrt) verwahren müssen oder nur einer Person übergeben dürfen, von der sie sicher sein konnte, dass diese Gewähr dafür bieten würde, dass es nicht zu einer Veröffentlichung kommt. Dass sie derart vorgesorgt hätte, hat sie nicht einmal behauptet.“

4.2.2 Oberster Gerichtshof in 6 Nc30/19t, Privat gg. Republik Österreich wegen Veröffentlichung eines OGH Disziplinarerkenntnisses im RIS

Mit **Beschluss vom 27.11.2019** zu Zl. 6Nc30/19t¹⁶ hat der **Oberste Gerichtshof** der Beschwerde eines Richters gegen die Veröffentlichung eines Disziplinarerkenntnisses des OGH im RIS nicht stattgegeben, in welchem dieser mit seinem richtigen Vornamen, dem richtigen Anfangsbuchstaben des Nachnamens und als Gatte der verfahrensführenden Richterin Mag. ***** im Strafverfahren gegen Mag. ***** erwähnt war, wobei seine Gattin als verfahrensführende Richterin ebenso medienwirksam bekannt sei, wie das laufende Disziplinarverfahren gegen ihn.

Der Beschwerdeführer machte im Wesentlichen geltend, dass er sich diskriminiert erachte, da in anderen Disziplinarerkenntnissen des Obersten Gerichtshofes ausreichende Anonymisierungen iS des § 133a RStDG (Veröffentlichung verfahrensbeendender Sachentscheidungen der Disziplinargerichte) vorgenommen worden seien, er im Recht auf Geheimhaltung personenbezogener, sensibler Daten verletzt worden sei (da auch die weltanschauliche bzw. politische Meinung aus ihm zurechenbaren Tweets hervorgingen) und die Weiterführung der Datenverarbeitung zumindest so eingeschränkt werden solle, dass sie dem Anonymisierungsgebot des § 133a des RStDG entspreche.

Begründung des OGH:

Zunächst hielt der OGH fest, dass eine ausdrückliche Regelung für Disziplinarverfahren im Gerichtsorganisationengesetz (GOG) fehlt. Da jedenfalls § 85a GOG (Datenschutz in Angelegenheiten der Strafgerichtsbarkeit) nicht anwendbar sei, richtet sich die Geltendmachung von datenschutzrechtlichen Ansprüchen im Zusammenhang mit einem Disziplinarverfahren nach **§ 85 GOG** (Datenschutz in Angelegenheiten der Gerichtsbarkeit in bürgerlichen Rechtssachen

¹⁶ https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20191127_OGH0002_0060NC00030_19T0000_000

und der weisungsfreien Justizverwaltung), wobei der zuständige **Senat des OGH entscheidungszuständig** sei.

Der OGH führt sodann im Wesentlichen aus, dass nach Art. 6 Abs. 1 lit. c DSGVO die Verarbeitung von Daten unter anderem dann **rechtmäßig sei, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist**, der der Verantwortliche unterliegt. Nach Art. 6 Abs. 1 lit. e DSGVO ist dies zudem dann der Fall, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Damit gelte weiterhin, dass eine den Verfahrensgesetzen entsprechende Verwendung von Daten auch aus datenschutzrechtlicher Sicht zulässig ist.

Gemäß § 133a RStDG seien rechtskräftige verfahrensbeendende Sachentscheidungen der Disziplinargerichte von der oder dem jeweiligen Vorsitzenden unverzüglich in anonymisierter Form **im RIS zu veröffentlichen**. Die Bestimmungen über die Entscheidungsdokumentation Justiz (§ 15 OGHG) seien sinngemäß anzuwenden (§ 133a Satz 2 RStDG).

Gemäß § 15 Abs. 4 OGHG seien in der Entscheidungsdokumentation Justiz Namen, Anschriften und erforderlichenfalls auch sonstige Orts- und Gebietsbezeichnungen, die Rückschlüsse auf die betreffende Rechtssache zulassen, durch Buchstaben, Ziffern oder Abkürzungen so zu anonymisieren, dass die Nachvollziehbarkeit der Entscheidung nicht verloren geht. **Für den Fall, dass Parteien oder sonstige Beteiligte durch identifizierende Sachverhaltsmerkmale in der Begründung, die zum Verständnis der Entscheidung erforderlich wären, erkennbar würden, ist eine Abwägung zwischen dem Interesse der Öffentlichkeit an der Information über höchstgerichtliche Entscheidungen und dem Anonymitätsinteresse der Beteiligten erforderlich.** Das Gesetz trifft dazu eine differenzierende Regelung: War das Verfahren in allen Instanzen ohne Durchführung einer öffentlichen Verhandlung zu führen, so kann der Senat nach § 15 Abs. 2 OGHG ein Unterbleiben der Veröffentlichung anordnen. Traf das nicht zu, so bleibt es bei der Grundregel des § 15 Abs. 1 OGHG; die Entscheidung sei daher auch dann zu veröffentlichen, wenn die Anonymität der Beteiligten nicht gewährleistet sei. Ein Weglassen (auch) des Vornamens und/oder des Anfangsbuchstabens des Familiennamens des Beschwerdeführers hätte demgegenüber zur Folge, dass damit auch der Bezug zu den festgestellten Tweets unter dem Account des Beschwerdeführers nicht ausreichend erkennbar wäre und damit die Tatsachengrundlage des Disziplinarerkenntnisses an Verständlichkeit einbüßen würde. Soweit der Beschwerdeführer argumentiert, durch die Veröffentlichung der Begründung des Disziplinarerkenntnisses seien sensible Daten offengelegt worden, weil darin davon die Rede ist, dass er und sein Sohn politisch interessiert, gesellschaftspolitisch *****orientiert und als solches auch kritisch gegenüber bestimmten Politikern bzw. Ex-Politikern eingestellt seien, ist ihm entgegenzuhalten, dass die diesbezüglichen Entscheidungspassagen ausschließlich die vom Beschwerdeführer selbst geposteten Tweets wiedergeben.

4.2.3 Parallele Zuständigkeit der Gerichte und Aufsichtsbehörden nach der DSGVO möglich (6 Ob 91/19d)

Der Oberste Gerichtshof hat den Revisionsrekurs von Facebook Ireland gegen die Entscheidung des Oberlandesgerichtes Wien (11 R 24/19h) vom 14.03.2019 (**M. S. gg. Facebook Ireland**) mit Beschluss vom 23.5.2019 (6 Ob 91/19d¹⁷) abgewiesen.

17 https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JIT_20190523_OGH0002_00600B00091_19D0000_000

Das OLG Wien hatte in seiner Entscheidung 11 R 24/19h – gegen den sich der Revisionsrekurs von Facebook richtete - festgestellt, **dass gemäß Art 79 Abs. 1 DSGVO jede betroffene Person unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Art 77 DSGVO das Recht auf einen wirksamen gerichtlichen Rechtsbehelf hat**, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung verletzt wurden.

Dagegen richtete sich der ordentliche Revisionsrekurs von Facebook Ireland, den der OGH abgewiesen hat.

Aus der Begründung:

- „In der **Literatur wird die Doppelgleisigkeit der Rechtsschutzmöglichkeiten weitgehend bejaht** (für Österreich Feiler/Forgó, EU-DSGVO Art 77 Rz 1; Jahnel in Krempelmeier/Staudinger/Weiser, Datenschutzrecht nach der DSGVO 43 ff). Demnach ist also nach Maßgabe der zitierten Bestimmungen das „One-Stop-Shop“-Prinzip gerade nicht (ausnahmslos) durchgehalten“
- „Im **Gesetzgebungsprozess auf europäischer Ebene hat Österreich als einziger Staat gegen die Verabschiedung der DSGVO gestimmt, weil durch die Parallelität der Rechtsschutzmöglichkeiten die Gefahr von sich widersprechenden gerichtlichen Entscheidungen in derselben Sache entstehe und eine Verletzung des Grundsatzes „res iudicata“ im Raum stehe** (Nemitz in Ehmann/Selmayr, DS-GVO2 Art 79 Rz 8 FN 4). **Gerade diese Episode der Gesetzwerdung spricht aber dafür, dass die DSGVO vom EU-Gesetzgeber gewollt eine Zweigleisigkeit des Rechtsschutzes normiert.** In welchem Verhältnis Art 77, 78 und Art 79 zueinander stehen, regelt die DSGVO nicht (Nemitz in Ehmann/Selmayr, DS-GVO2 Art 79 Rz 8).“
- „Dies könnte im vorliegenden Fall dafür sprechen, dass die vom Kläger geltend gemachten Feststellungsbegehren auch in einem Verfahren vor der Aufsichtsbehörde geltend gemacht werden könnten. Daraus ist aber für den Rechtsstandpunkt der Beklagten nichts zu gewinnen, **weil dem EU-Recht auch Vorrang vor der Verfassung der Mitgliedstaaten zukommt.** Dabei bedarf es im vorliegenden Fall keines Eingehens auf die Frage, ob das österreichische Verfassungsrecht einen integrationsfesten Kern aufweist (vgl Mayer/Kuscko-Staydlmayer/Stöger, Bundesverfassungsrecht11 246/10), weil der Umstand, dass dem Kläger gegebenenfalls mehrere Rechtsschutzmöglichkeiten bei verschiedenen innerstaatlichen Stellen offenstehen, wobei jedoch jeweils eine nachprüfende Kontrolle der Entscheidung durch unabhängige Gerichte gewährleistet ist, jedenfalls keine Verletzung eines derartigen unverzichtbaren Kerns des österreichischen Verfassungsrechts darstellt.“

4.2.4 Videoaufnahmen im Lichte der §§ 12, 13 DSG (6 Ob 150/19f)

Der Oberste Gerichtshof hat am 27.11.2019 zu Zl. 6 Ob 150/19f der Revision gegen das Urteil des LG Salzburg als Berufungsgericht nicht Folge gegeben.

Hintergrund:

Der Kläger beehrte die Entfernung und die Unterlassung der Anbringung einer schwenkbaren Überwachungskamera, die insbesondere einen Teil des vom Kläger bewohnten Gartens und den allgemein zugänglichen Weg vor den Gärten erfasst, da ein ständiger Überwachungsdruck vorliege, die Überwachung den Kläger und seine Familie in ihrem Grundrecht auf Privatsphäre und in ihrem Recht am eigenen Bild verletzte und darüber hinaus auch die Bestimmungen des Datenschutzgesetzes nicht eingehalten wären.

Das Berufungsgericht gab dem Klagebegehren statt und sprach aus, dass die ordentliche Revision zulässig ist; es fehle Rechtsprechung des Obersten Gerichtshofs zur Anwendbarkeit „der neuen Rechtsordnung“ (gemeint: des Datenschutzgesetzes idF des Datenschutz-Anpassungsgesetzes 2018, BGBl I 2018/120);

Begründung:

Der OGH sah im vorliegenden Fall die Voraussetzungen zur Anwendbarkeit der DSGVO als gegeben an, verneinte die Anwendung des Haushaltsprivilegs gemäß Art. 2 Abs. 2 lit. c DSGVO, das restriktiv auszulegen und bei Aufnahmen zur Beweissicherung nicht zur Anwendung komme.

In einem weiteren Schritt prüfte der OGH das Vorliegen der Voraussetzungen des Art. 6 Abs. 1 lit. f DSGVO, nämlich Vorliegen eines berechtigten Interesses zur Verarbeitung, Erforderlichkeit der Verarbeitung zur Verwirklichung dieses Interesses und kein Überwiegen der Grundrechte und Grundfreiheiten der betroffenen Person.

Danach führt der OGH zur Anwendbarkeit der §§ 12, 13 DSG folgendes an:

*„Das Datenschutzgesetz idF des Datenschutz-Anpassungsgesetzes 2018 (BGBl I 2018/120) enthält im **Gegensatz zur DSGVO explizite Bestimmungen zur Bildverarbeitung, weshalb im Folgenden (auch) auf §§ 12 und 13 DSG näher einzugehen ist** (vgl auch Knyrim, DatKomm Vorbemerkung Entwicklung des österreichischen DSG und aktuelle Rechtsentwicklung im Datenschutzrecht Rz 13). (...) In § 12 Abs. 3 DSG **wird die Interessenabwägung bereits auf gesetzlicher Ebene für „quasi massenhaft auftretende Fallkonstellationen“ vorgenommen** (Kastelitz/Hötzendorfer/Tschohl aaO Rz 85). Es sind dies (beispielhafte) Fälle, in denen die Bildaufnahme „insbesondere“ zulässig ist, wobei hier lediglich § 12 Abs. 3 Z 1 und 2 DSG Anwendung finden könnte. Gemäß § 12 Abs. 3 Z 1 DSG ist eine Bildaufnahme gemäß § 12 Abs. 2 Z 4 DSG dann zulässig, wenn sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen.“*

Im Ergebnis kommt der OGH zum Schluss, dass die Überwachungsmaßnahme des Beklagten im Rahmen der vorzunehmenden Interessenabwägung überschießend war, der Beklagte kein berechtigtes Interesse habe, zu erfahren, wann und wie oft der Kläger und dessen Familie den Zugangsweg und den Eckbereich des eigenen Gartens benützen, und die Videoüberwachung hinsichtlich eines Teils der festgestellten Handlungen tatsächlich auch nicht geeignet sei, Störungshandlungen zu unterbinden (zB hinsichtlich Belästigungen beim Spazierengehen).

4.3 Verwaltungsgerichtshof

4.3.1 VwGH, Ra 2017/04/0141, 17. Dezember 2019

Im vorliegenden Fall ist der Beschwerdegegner ein Gemeindeverband. Dieser betreibt ein Krankenhaus, in dem die Beschwerdeführerin angestellt war. Die Beschwerdeführerin unterzog sich in diesem Krankenhaus auch einer Operation, weshalb ihre Gesundheitsdaten im elektronischen Patientendokumentationssystem („Patidok“) des Krankenhauses gespeichert waren. Die Beschwerdeführerin behauptete nun in ihrer Beschwerde an die Datenschutzbehörde (DSB), dass der Verwaltungsdirektor dieses Krankenhauses, der zugleich ihr dienstlicher Vorgesetzter war, unzulässigerweise auf ihre Gesundheitsdaten in „Patidok“ zugegriffen habe. Die Beschwer-

deführerin brachte dazu vor, dass der Verwaltungsdirektor überhaupt nicht berechtigt sei, ihre Gesundheitsdaten abzufragen.

Die DSB wies diese Beschwerde zurück und begründete dies damit, dass die Sache bereits von der Datenschutzbehörde entschieden worden und nunmehr beim Bundesverwaltungsgericht (BVwG) anhängig sei. Weitere Rechtsverletzungen habe die Beschwerdeführerin – trotz Nachfrage der DSB – nicht konkretisiert. Die Frage, ob der Verwaltungsdirektor aufgrund der ihm konkret übertragenen Aufgaben überhaupt auf Gesundheitsdaten der Beschwerdeführerin zugreifen dürfe, sei nicht geeignet, im Rahmen eines Verfahrens nach § 31 Abs. 1 DSG 2000 („Beschwerde an die Datenschutzbehörde“) behandelt zu werden.

Die Beschwerdeführerin erhob gegen den zurückweisenden Bescheid der DSB Beschwerde an das BVwG. Das BVwG wies diese Beschwerde ab.

Die Beschwerdeführerin erhob auch gegen das Erkenntnis des BVwG außerordentliche Revision an den Verwaltungsgerichtshof (VwGH) und begründete dies damit, dass keine Rechtsprechung des VwGH zur „inhaltlichen Determinierung von Beschwerden nach § 31 DSG 2000“ bestehe.

Der VwGH wies die außerordentliche Revision zurück und begründete dies damit, dass keine Rechtsfrage von grundsätzlicher Bedeutung vorliege. (Das Vorliegen einer Rechtsfrage von grundsätzlicher Bedeutung ist aber Voraussetzung dafür, dass sich der VwGH inhaltlich mit einer Revision auseinandersetzt). Der VwGH führte weiter aus, dass das bloße Fehlen von Rechtsprechung des VwGH dann keine Rechtsfrage von grundsätzlicher Bedeutung aufwerfe, wenn die Rechtslage – wie hier – eindeutig sei und keiner Klärung bedürfe. Auch seien die Vorgaben zur Einbringung einer Beschwerde gemäß § 31 DSG 2000 ohnehin detailliert.

4.3.2 VwGH, Ra 2017/04/0145; 30.04.2019

Die selbe Beschwerdeführerin brachte in ihrer Beschwerde bei der DSB vor, in ihrem Recht auf Geheimhaltung verletzt zu sein, weil ihre Krankenunterlagen trotz Widerrufs ihrer Zustimmung zur Verarbeitung ihrer Daten in „Patidok“ abrufbar seien. Die DSB wies die Beschwerde ab und begründete dies damit, dass keine Verletzung im Recht auf Geheimhaltung vorliege, wenn ein Gesetz zur Verwendung dieser Daten – hier Gesundheitsdaten – ermächtige oder verpflichte. Im vorliegenden Fall gäbe es ein solches Gesetz (§ 15 Tiroler Krankenanstaltengesetz).

Das BVwG bestätigte den Bescheid der DSB.

Der VwGH wies die außerordentliche Revision der Beschwerdeführerin mangels Rechtsfrage von grundsätzlicher Bedeutung ab. Unter anderem sprach der VwGH – wie schon die DSB und das BVwG – aus, dass es nicht auf die Zustimmung und demnach nicht auf den Widerruf der Zustimmung zur Verwendung der Gesundheitsdaten der Beschwerdeführerin ankomme, wenn ein Gesetz – wie hier – die Datenverwendung rechtfertige. Auch die von der Beschwerdeführerin aufgeworfene Rechtsfrage, ob die erkennende Richterin, die das angefochtene Erkenntnis des BVwG erlassen habe, deshalb befangen sei, weil sie bis zu ihrer Ernennung als Richterin für die DSB gearbeitet habe, wies der VwGH zurück. Der bloße Umstand, dass eine Richterin nun über Beschwerden gegen Bescheide ihrer „ehemaliger Kollegen“ bei der DSB entscheide, sei nicht ausreichend, den Anschein ihrer Unabhängigkeit und Unparteilichkeit zu beeinträchtigen. Dass dieser Anschein der Unabhängigkeit beeinträchtigt werde, müssten besondere Gründe vorliegen. Diese lagen aber hier nicht vor.

4.3.3 VwGH, Ra 2017/04/0134, 30. April 2019

Ein Beschwerdeführer brachte bei der DSB eine Beschwerde wegen Nicht-Erteilung einer Auskunft ein. Der Beschwerdegegner ist Anwalt und vertritt einen Mandanten, mit dem der Beschwerdeführer in einen Rechtsstreit verwickelt war. Die DSB gab der Beschwerde statt, weil sich der Anwalt im Beschwerdeverfahren vor der DSB pauschal auf seine Verschwiegenheitspflicht berief, aber dem Beschwerdeführer nicht auf seinen Antrag auf Auskunft antwortete. Unter einem trug die DSB dem Beschwerdegegner auf, dem Auskunftsbegehren nachzukommen oder schriftlich zu begründen, warum die Auskunft nicht oder nicht vollständig erteilt werden könne.

Das BVwG bestätigte den Bescheid der DSB.

Der Beschwerdeführer brachte eine außerordentliche Revision gegen das Erkenntnis des BVwG ein und begründete das Vorliegen einer Rechtsfrage von grundsätzlicher Bedeutung damit, dass Rechtsprechung des VwGH zum Verhältnis der Verschwiegenheitsverpflichtung gemäß § 9 Abs. 2 RAO und der Auskunftspflicht gemäß § 26 DSG 2000 fehle.

Der VwGH wies die außerordentliche Revision mangels Vorliegens einer Rechtsfrage von grundsätzlicher Bedeutung zurück. Er begründete dies damit, dass die DSB und das BVwG eine Verletzung des Auskunftsrechts des Beschwerdeführers angenommen hätten, weil der Anwalt dem Beschwerdeführer nicht direkt geantwortet hatte. Es komme hier also gar nicht auf das Verhältnis der Verschwiegenheitsverpflichtung und der Auskunftspflicht an, weil der Anwalt dem Beschwerdeführer jedenfalls antworten müsse, selbst wenn er in der Antwort nur begründe, warum die Auskunft nicht oder nicht vollständig erteilt werden könne. Außerdem läge auch deshalb keine Rechtsfrage von grundsätzlicher Bedeutung vor, weil im angefochtenen Erkenntnis die alte datenschutzrechtliche Rechtslage angewendet worden sei, die bereits am 24. Mai 2018 außer Kraft getreten sei und voraussichtlich nur mehr wenige Personen betreffe.

4.3.4 VwGH, Ra 2018/04/0194, 22. März 2019

Ein Einschreiter behauptete, durch Abbildungen, die ein gerichtlich beeideter Sachverständiger von ihm und seinem PKW gemacht habe, in seinem Recht auf Geheimhaltung verletzt worden zu sein ersuchte die DSB, „das diesbezügliche Verwaltungsverfahren einzuleiten“. Weiters sei ihm - so der Einschreiter weiter - empfohlen worden, die belangte Behörde „um bescheidmäßige Feststellung zu ersuchen“. Die DSB führte in diesem Fall kein bescheidmäßiges Beschwerdeverfahren, da – nach der hier anzuwendenden Rechtslage gemäß DSG 2000 – für Verletzungen im Recht auf Geheimhaltung durch Private (hier: der gerichtliche Sachverständige) nicht die DSB, sondern die Zivilgerichte zuständig waren. Die DSB führte stattdessen ein Kontroll- und Ombudsmannverfahren nach § 30 DSG 2000, das nicht mit einem förmlichen Bescheid, sondern mit einer formlosen Einstellung oder Empfehlung endete. Im Hinblick auf das Ersuchen um bescheidmäßige Feststellung teilte die DSB dem Einschreiter mit, dass für die Feststellung einer Verletzung im Recht auf Geheimhaltung durch einen Privaten die Zivilgerichte zuständig seien, weshalb sie davon ausgehe, dass das gegenständliche Kontroll- und Ombudsmannverfahren eingestellt werden könne.

Der Einschreiter erhob in Folge Säumnisbeschwerde an das BVwG, weil die DSB seinen Fall nicht mittels Bescheid entschieden hatte.

Das BVwG erachtete die Säumnisbeschwerde als zulässig. Das BVwG begründete dies damit, dass die DSB den Antrag des Einschreiters zumindest wegen Unzuständigkeit zurückweisen hätte müssen, auch wenn sie zum damaligen Zeitpunkt (vor Inkrafttreten der DSGVO) nicht zuständig gewesen sei, Verletzungen im Recht auf Geheimhaltung durch Private zu verfolgen.

Die DSB erhob gegen dieses Erkenntnis des BVwG Amtsrevision und begründete dies damit, dass nicht klar sei, warum das BVwG hier von einem Antrag zur bescheidmäßigen Feststellung im Sinn des § 13 AVG ausgehe.

Der VwGH wies die Amtsrevision mangels Rechtsfrage von grundsätzlicher Bedeutung zurück. Er verwies dabei auf seine Judikatur, wonach die in vertretbarer Weise vorgenommene einzel-fallbezogene Auslegung von Parteierklärungen nur dann mittels Revision anfechtbar (revisibel) sei, wenn dem BVwG eine krasse Fehlbeurteilung unterlaufen wäre. Von einer solch krasen Fehlbeurteilung des BVwG bei der Auslegung der Eingabe des Einschreiters, er habe hinsichtlich der behaupteten Verletzung im Recht auf Geheimhaltung einen bescheidmäßigen Anspruch begehrt, sei aber nicht auszugehen.

4.4 Europäischer Gerichtshof für Menschenrechte

4.4.1 EGMR, *Catt v. the United Kingdom*, 24.01.2019 – 43514/15

Dieser Fall betraf die Beschwerde eines lebenslangen Aktivisten, über die Erhebung und Speicherung seiner personenbezogenen Daten in einer Polizeidatenbank für inländische Extremisten.

Der EGMR hielt fest, dass ein Verstoß gegen Art. 8 EMRK vorlag, da die über den Kläger gespeicherten Daten seine politischen Ansichten betrafen und diese Informationen eines besonderen Schutzes bedurften. Der EGMR berücksichtigte das Alter des Klägers (94) und die Tatsache, dass er keine Vorgeschichte im Hinblick auf Gewalttaten hatte. Er stellte ferner fest, dass die Erhebung der Informationen über den Kläger zwar gerechtfertigt gewesen war, nicht jedoch ihre umfangreiche Aufbewahrung, insbesondere wegen fehlender Schutzmaßnahmen wie etwa Fristen.

4.4.2 EGMR, *López Ribalda and Others v. Spain*, 17.10.2019 – 1874/13 und 8567/13

In diesem Fall ging es um die verdeckte Videoüberwachung von Mitarbeitern, aufgrund eines Diebstahlsverdachts, die in weiterer Folge zu deren Entlassung führte. Die Kläger beschwerten sich über die verdeckte Videoüberwachung und die Verwendung der gewonnenen Daten durch die spanischen Gerichte zur Feststellung, dass ihre Entlassung zu Recht erfolgte. Überdies beschwerten sich die Kläger, welche auch Vergleichsvereinbarungen unterzeichnet hatten, dass diese Vereinbarungen, aufgrund des Videomaterials, unter Zwang getroffen wurden und von den Gerichten nicht als Beweis für die Fairness ihrer Entlassungen hätten akzeptiert werden dürfen.

Der EGMR stellte fest, dass bei den fünf Klägern keine Verletzung von Art. 8 EMRK vorlag. Er stellte weiters fest, dass die spanischen Gerichte die Rechte der Kläger und jene des Arbeitgebers sorgfältig gegeneinander abgewogen und die Rechtfertigung der Videoüberwachung eingehend geprüft hatten. Ein wesentliches Argument der Kläger war, dass sie nicht vorab über die Überwachung informiert wurden, doch hielt der EGMR hierzu fest, dass die verdeckte Videoüberwachung aufgrund eines begründeten Verdachts auf schwerwiegendes Fehlverhalten, unter Berücksichtigung des Umfangs und der Folgen der getroffenen Maßnahme, gerechtfertigt gewesen sei. Im vorliegenden Fall hätten die inländischen Gerichte somit ihren Ermessensspielraum bei der Feststellung der Verhältnismäßigkeit und Rechtmäßigkeit der Überwachung nicht überschritten. Der EGMR stellte ferner fest, dass kein Verstoß gegen Art. 6 Abs. 1 EMRK

vorlag und die Verwendung des Videomaterials als Beweismittel die Fairness des Verfahrens nicht untergraben hatte.

4.4.3 EGMR, Hambardzumyan v. Armenia, 05.12.2019 – 43478/11

Die Klägerin behauptete in diesem Fall, dass die Polizei keinen gültigen Gerichtsbeschluss gehabt habe, um sie während einer strafrechtlichen Untersuchung unter geheime Überwachung zu stellen. Sie beschwerte sich insbesondere über die verdeckte Überwachung und deren anschließende Verwendung im Strafverfahren gegen sie.

Der EGMR stellte eine Verletzung von Art. 8 EMRK fest, da die angewandte Überwachungsmaßnahme keiner ordnungsgemäßen richterlichen Aufsicht unterstellt und daher nicht gesetzeskonform im Sinne der Konvention war. Der EGMR hielt hierzu fest, dass der Gerichtsbeschluss nicht spezifisch genug war, insbesondere in Bezug auf die Person, die Gegenstand der Überwachungsmaßnahme sein sollte. Bei solch schwerwiegendem Eingriff in das Recht auf Achtung des Privat- und Familienlebens, wie dies etwa eine geheime Überwachung darstellt, ist dies nach Ansicht des EGMR jedenfalls nicht akzeptabel. Des Weiteren habe der Gerichtsbeschluss nicht die konkreten Maßnahmen angeführt, die gegen die Klägerin durchzuführen seien. Der EGMR stellte weiters fest, dass im Fall der Klägerin kein Verstoß gegen Art. 6 EMRK vorlag und, dass die Verwendung des heimlich aufgenommenen Materials nicht im Widerspruch zu den durch Art. 6 Abs. 1 leg. cit. garantierten Anforderungen der Fairness stand.

4.5 Europäischer Gerichtshof

4.5.1 Urteil vom 14. Februar 2019, C-345/17 (Buivids)

Mit Urteil vom 14. Februar 2019 befasste sich der EuGH auf Vorlage der Augstākā tiesa (Oberster Gerichtshof, Lettland) mit dem Spannungsverhältnis zwischen dem Recht auf Schutz personenbezogener Daten nach Art. 8 EU-GRC und dem Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit nach Art. 11 EU-GRC.

Herr Buivids fertigte im Rahmen seiner polizeilichen Einvernahme ein Video an, welches die Polizeibeamten und deren Tätigkeit auf der Polizeidienststelle zeigte und veröffentlichte dieses Video in weiterer Folge auf der Video-Plattform www.youtube.com. Im Verfahren vor dem EuGH ging es um die Frage der Zulässigkeit der Veröffentlichung eines solchen Videos auf Grundlage von Art. 7 lit. f der Richtlinie 95/46/EG (nunmehr: Art. 6 Abs. 1 lit. f DSGVO).

Der EuGH verwies zunächst darauf, dass die Aufzeichnung und Veröffentlichung eines solchen Videos nicht unter die (nunmehr in Art. 2 Abs. 2 lit. c DSGVO) normierte „Haushaltsausnahme“ falle. Dies deshalb, da Herr Buivids das in Rede stehende Video auf einer öffentlich zugänglichen Video-Plattform veröffentlicht habe. Darüber hinaus sei keine Ausnahme vorgesehen, wonach Beamte vom Anwendungsbereich der Richtlinie 95/46/EG ausgenommen werden würden.

Im Hinblick auf die Frage der Zulässigkeit der Veröffentlichung verwies der EuGH auf die Rechtsprechung des EGMR, wonach bei der Interessenabwägung nach Art. 7 lit. f der Richtlinie 95/46/EG folgende Faktoren zu berücksichtigen seien: Der Beitrag zu einer Debatte von allgemeinem Interesse, der Bekanntheitsgrad der betroffenen Person, der Gegenstand der Berichterstattung, das vorangegangene Verhalten der betroffenen Person, Inhalt, Form und Auswirkungen der Veröffentlichung, die Art und Weise sowie die Umstände, unter denen die Informationen erlangt worden sind, und deren Richtigkeit.

Die Durchführung der konkreten Interessenabwägung überließ der EuGH allerdings dem vorlegenden Gericht, da der Sachverhalt weiter klärungsbedürftig sei, insbesondere in Bezug auf die Frage, ob mit der Veröffentlichung des Videos das ausschließliche Ziel verfolgt wurde, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten.¹⁸

4.5.2 Urteil vom 29. Juli 2019, C-40/17 (Fashion ID)

Mit Urteil vom 29. Juli 2019 befasste sich der EuGH auf Vorlage des Oberlandesgerichtes Düsseldorf (Deutschland) insbesondere mit dem Begriff des Verantwortlichen nach Art. 2 lit. d der Richtlinie 95/46/EG (nunmehr: Art. 4 Z 7 DSGVO).

Das Verfahren dreht sich im Kern um die Frage der Beurteilung der datenschutzrechtlichen Rollenverteilung für den Fall, dass der Betreiber einer Webseite ein Social-Plugin eines anderen Anbieters einbindet und es durch diese Einbindung – vereinfacht formuliert – zur Übermittlung personenbezogener Daten des Besuchers der Webseite an diesen Anbieter kommt.

Der EuGH hielt fest, dass der Betreiber einer Webseite, der sich dazu entscheidet, ein Social-Plugin eines Dritten einzubauen, als gemeinsam Verantwortlicher mit diesem Dritten zu qualifizieren sei. Diesbezüglich führte der EuGH unter Verweis auf seine bisherige Rechtsprechung aus, dass es für die gemeinsame Verantwortlichkeit nicht darauf ankomme, dass jeder Verantwortliche auch Zugang zu den betreffenden personenbezogenen Daten habe. Im konkreten Fall würden der Betreiber der Webseite und der Dritte die „Zwecke und Mittel“ (Implementierung eines „Gefällt mir“-Buttons im Wissen, dass dieser als Werkzeug für die Verarbeitung personenbezogener Daten dient) festlegen.

Die gemeinsame Verantwortlichkeit sei jedoch auf den Vorgang oder die Vorgänge beschränkt, für den bzw. für die der Betreiber der Webseite tatsächlich über die Zwecke und Mittel entscheidet. Dies sei im konkreten Fall das Erheben der personenbezogenen Daten und deren Weitergabe (ermöglicht durch die Implementierung des „Gefällt mir“-Buttons).

4.5.3 Urteil vom 24. September 2019, C-507/17 (Google LLC gg. CNIL)

Mit Urteil vom 24. September 2019 befasste sich der EuGH auf Vorlage des Conseil d'État (Staatsrat, Frankreich) mit der räumlichen Tragweite des Rechts auf Auslistung von Suchergebnissen nach Art. 12 lit. b und Art. 14 Abs. 1 lit. a der Richtlinie 95/46/EG (nunmehr: Art. 17 DSGVO, „Recht auf Vergessenwerden“).

Das Verfahren dreht sich im Kern um die Frage, wie Google als Suchmaschinenbetreiber vorzugehen hat, wenn ein entsprechender Antrag einer betroffenen Person darauf gerichtet ist, Links aus den Suchergebnissen zu entfernen, die anlässlich einer Suche anhand des Namens der betroffenen Person angezeigt werden. Während Google seitens der französischen Aufsichtsbehörde (CNIL) angewiesen wurde, die beantragte Auslistung auf sämtliche Domains (also alle Versionen) seiner Suchmaschine anzuwenden, vertrat Google den Standpunkt, dass die Ergebnisse nur in allen mitgliedstaatlichen Versionen auszulisten seien.

Der EuGH verwies zunächst darauf, dass Google als Suchmaschinenbetreiber verpflichtet sei, einem berechtigten Antrag nachzukommen und dass diesfalls Links aus Suchergebnissen zu entfernen seien, die anlässlich einer Suche anhand des Namens der betroffenen Person angezeigt werden würden. Im Hinblick auf die Tragweite des „Rechts auf Auslistung von Sucher-

18 Der OGH hatte sich mit Urteil vom 27. Juni 2019, 6 Ob 6/2019 mit einem ähnlich gelagerten Fall zu befassen; siehe dazu Punkt 4.2.

gebnissen“ hielt der EuGH jedoch fest, dass die Verpflichtung nicht weltweit gelte und dass die Auslistungspflicht auf das Hoheitsgebiet der Union (also auf alle mitgliedstaatlichen Versionen von Google) beschränkt sei.

Als Begründung führte der EuGH im Wesentlichen ins Treffen, dass Drittstaaten unter Umständen kein „Auslistungsrecht“ kennen würden. Darüber hinaus sei das Recht auf Schutz personenbezogener Daten kein uneingeschränktes Recht und müsse dieses im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden, wobei eine solche Abwägung weltweit unterschiedlich ausfallen könne. Daraus folge, dass (nach derzeitigem Stand) ein Suchmaschinenbetreiber, der einem Auslistungsantrag der betroffenen Person – gegebenenfalls auf Anordnung einer Aufsichts- oder Justizbehörde eines Mitgliedstaats – stattgebe, nicht aus dem Unionsrecht verpflichtet sei, eine solche Auslistung in allen Versionen seiner Suchmaschine vorzunehmen.

Darüber hinaus wurde festgehalten, dass Suchmaschinenbetreiber sehr wohl verpflichtet seien, hinreichend wirksame Maßnahmen zu ergreifen, um einen wirkungsvollen Schutz der Grundrechte der betroffenen Person sicherzustellen. Diese Maßnahmen müssten ihrerseits alle gesetzlichen Anforderungen erfüllen und bewirken, dass die Internetnutzer in den Mitgliedstaaten daran gehindert oder zumindest zuverlässig davon abgehalten werden würden, auf die betreffenden Links über eine Suche anhand des Namens der betroffenen Person zuzugreifen.

Schließlich wurde festgehalten, dass zwar das Unionsrecht – wie oben ausgeführt – eine Auslistung aus allen Versionen der Suchmaschine nicht vorschreibe, das Unionsrecht dies allerdings auch nicht verbiete. Die Aufsichts- oder Justizbehörden eines Mitgliedstaats seien daher befugt, anhand von nationalen Schutzstandards für Grundrechte eine Abwägung zwischen dem Recht der betroffenen Person auf Achtung des Privatlebens und auf Schutz der sie betreffenden personenbezogenen Daten einerseits und dem Recht auf freie Information andererseits vorzunehmen und nach erfolgter Abwägung gegebenenfalls den Suchmaschinenbetreiber anzuweisen, eine Auslistung in allen Versionen seiner Suchmaschine vorzunehmen.

4.5.4 Urteil vom 24. September 2019, C-136/17 (GC u.a gg. CNIL)

Mit Urteil vom 24. September 2019 befasste sich der EuGH auf Vorlage des Conseil d'État (Staatsrat, Frankreich) mit den Pflichten eines Suchmaschinenbetreibers im Zusammenhang mit besonderen Kategorien personenbezogener Daten nach Art. 8 Abs. 1 der Richtlinie 95/46/EG bzw. nach nunmehr Art. 9 Abs. 1 DSGVO.

Das Verfahren dreht sich im Kern um die Frage, ob und inwiefern das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten (mit Erlaubnisvorbehalt) auch auf Suchmaschinenbetreiber anwendbar ist und weiters, ob Informationen über ein Gerichtsverfahren zu den Datenkategorien „strafrechtliche Verurteilungen und Straftaten“ zählen.

Der EuGH bejahte die Anwendbarkeit des Verbots der Verarbeitung besonderer Kategorien personenbezogener Daten für Suchmaschinenbetreiber: Zwar seien Suchmaschinenbetreiber nicht für die Daten verantwortlich, die auf der Webpage von Dritten vorhanden seien, sehr wohl aber für die Listung dieser Webpage und insbesondere für die Anzeige (samt den damit verbundenen Informationen) des auf die Webpage führenden Links in der Ergebnisliste.

Darüber hinaus hielt er fest, dass Suchmaschinenbetreiber zur Auslistung verpflichtet seien, sofern keine Ausnahme nach nunmehr Art. 9 Abs. 1 DSGVO vorhanden sei. Es müsse insbesondere geprüft werden, ob die Aufnahme des Links in die Ergebnisliste erforderlich sei, um das Recht auf freie Information gemäß Art. 11 EU-GRC auszuüben, welches den Internetnutzern

zustehe. Zwar würden die Rechte nach Art. 7 und Art. 8 EU-GRC grundsätzlich gegenüber dem Recht auf freie Information überwiegen, die Interessenabwägung könne allerdings je nach den Umständen des Einzelfalls variieren.

Schließlich hielt der EuGH fest, dass Informationen über ein (Straf-) Gerichtsverfahren zu den Datenkategorien „strafrechtliche Verurteilungen und Straftaten“ zählen würden. Es sei nicht relevant, ob die Begehung der Straftat im Zuge des Verfahrens tatsächlich festgestellt wurde. Einem Antrag auf Auslistung sei (auch) stattzugeben, wenn sich die Information auf einen früheren Abschnitt des Gerichtsverfahrens beziehe und diese Information nicht mehr die aktuelle Situation wiedergebe; anderes könne wiederum gelten, wenn im Einzelfall das Recht auf freie Information gegenüber dem Recht des Einzelnen auf Achtung des Privatlebens und auf Schutz personenbezogener Daten überwiegen würde (etwa zur Nachvollziehbarkeit des Ablaufs eines Gerichtsverfahrens).

4.5.5 Urteil vom 1. Oktober 2019, C-673/17 (Planet 49)

Mit Urteil vom 1. Oktober 2019 befasste sich der EuGH auf Vorlage des Bundesgerichtshofes (Deutschland) mit den Anforderungen an das Setzen von Cookies im Zusammenhang mit der Bestimmung nach Art. 5 Abs. 3 der Richtlinie 2002/58/EG (in der Fassung der Richtlinie 2009/136/EG).

Das Verfahren dreht sich im Kern um die Frage, ob eine wirksame Einwilligung durch bereits vorangekreuzte Kästchen abgegeben wird.

Der EuGH hielt diesbezüglich fest, dass das Erfordernis einer „Willensbekundung“ nach dem Wortlaut von Art. 5 Abs. 3 der Richtlinie 2002/58/EG iVm Art. 2 lit. h der Richtlinie 95/46/EG auf ein aktives und kein passives Verhalten hindeute. Ein vorangekreuztes Kästchen deute jedoch auf kein aktives Verhalten des Webpage-Nutzers hin. In diesem Zusammenhang verwies der EuGH auch auf ErwGr. 32 (der nunmehr geltenden) DSGVO, in dem explizit auf „vorangekreuzte Kästchen“ Bezug genommen und klargestellt wird, dass solche keine Einwilligung darstellen. Im Ergebnis ging der EuGH somit (erwartungsgemäß) davon aus, dass eine wirksame Einwilligung nicht durch bereits vorangekreuzte Kästchen abgegeben wird.

Im Rahmen des gegenständlichen Verfahrens hielt der EuGH zudem fest, dass die Bestimmung nach Art. 5 Abs. 3 der Richtlinie 2002/58/EG den Nutzer vor jedem Eingriff (gegenständlich: das Setzen von Cookies) in seine Privatsphäre schützen soll, unabhängig davon, ob dabei personenbezogene Daten oder andere Daten betroffen sind. Ausgehend von dieser Überlegung des EuGH geht der Anwendungsbereich von Art. 5 Abs. 3 der Richtlinie 2002/58/EG („Eingriff in die Privatsphäre“) somit über jenen der DSGVO hinaus, der gemäß Art. 2 Abs. 1 DSGVO auf die Verarbeitung von personenbezogenen Daten beschränkt ist.

4.5.6 Urteil vom 11. Dezember 2018, C-708/18 (TK)

Mit Urteil vom 11. Dezember 2018 befasste sich der EuGH auf Vorlage des Tribunal București (Landgericht Bukarest, Rumänien) mit der Frage der datenschutzrechtlichen Zulässigkeit einer Videoüberwachung, deren Aufnahmebereich (auch) den Gemeinschaftsbereich eines Wohngebäudes erfasst.

Das Verfahren dreht sich im Kern um die Frage, ob Art. 6 Abs. 1 lit. c und Art. 7 lit. f („berechtigzte Interessen“) der Richtlinie 95/46 derart auszulegen sind, dass sie nationalen Vorschriften entgegenstehen, wonach es zulässig ist, ohne Einwilligung der betroffenen Personen ein derartiges

Videoüberwachungssystem einzurichten, um berechtigte Interessen in Form des Schutzes und der Sicherheit von Personen und Eigentum zu gewährleisten.

Der EuGH hat festgehalten, dass Art. 7 lit. f der Richtlinie 95/46 einen Mitgliedstaat daran hindere, kategorisch und ganz allgemein die Verarbeitung bestimmter Kategorien personenbezogener Daten auszuschließen, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen. Ein Mitgliedstaat könne daher für diese Kategorien das Ergebnis der Abwägung der einander gegenüberstehenden Rechte und Interessen nicht abschließend vorschreiben, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfallen könnte.

Darüber hinaus enthalte Art. 7 der Richtlinie 95/46 eine abschließende Liste der Fälle, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden könnten. Die Mitgliedstaaten dürften weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben diesem Artikel einführen noch zusätzliche Bedingungen stellen, die die Tragweite eines der sechs darin vorgesehenen Grundsätze verändern würden.

Im Hinblick auf die konkret durchzuführende Interessenabwägung hat der EuGH festgehalten, dass ein „berechtigtes Interesse“ zum Zeitpunkt der Verarbeitung entstanden und vorhanden sein müsse und zu diesem Zeitpunkt nicht hypothetisch sein dürfe. Es könne bei der Beurteilung aller Umstände des jeweiligen Falles allerdings nicht zwingend verlangt werden, dass die Sicherheit des Eigentums und der Personen zuvor beeinträchtigt wurde.

5 Datenschutz-Grundverordnung und Datenschutzgesetz – Erfahrungen und legislative Maßnahmen

5.1 Erfahrungen der DSB im Berichtszeitraum

5.1.1 Verfahrenszahlen und Personalstand

Der massive Anstieg der Verfahrenszahlen hat sich im Jahr 2019 fortgesetzt.

In allen Bereichen kam es zu einer Steigerung der anhängig gemachten Verfahren, eine Trendwende ist nicht in Sicht. Ein Gutteil der Beschwerdeverfahren betrifft die Österreichische Post AG, sodass die DSB derzeit 1,5 Vollzeitäquivalente für die Bearbeitung dieser Beschwerdeverfahren einsetzen muss.

Der Personalstand der DSB kann mit dieser Steigerung nicht Schritt halten. Im Jahr 2018 wurden der DSB insgesamt 6 Planstellen des höheren Dienstes zugeteilt.

Es war möglich, im Berichtszeitraum vier Verwaltungspraktikanten aufzunehmen, die den Personalengpass punktuell abfedern konnten. Da es sich bei einem Verwaltungspraktikum um ein Ausbildungsverhältnis handelt, das längstens 12 Monate dauert, ist dies eine kurzfristige Maßnahme, die eine Erhöhung des Personalstandes nicht zu kompensieren vermag.

Auch die Anordnung von Mehrdienstleistungen, wie im Berichtszeitraum erfolgt, kann nur als vorübergehende Maßnahme und nicht als Dauerlösung angesehen werden.

Weiters führten die gestiegenen Verfahrenszahlen auch zu Rückständen in der Kanzlei, was sich in verzögerten Protokollierungen und Abfertigungen bemerkbar machte. Zeitweise betrug der Rückstand bis zu 4 Wochen.

Die steigenden Verfahrenszahlen, gepaart mit dem derzeitigen Personalstand, bedingen, dass die Verfahrensdauer, die von Gesetzes wegen längstens 6 Monate betragen sollte, in etlichen Fällen überschritten wurde. Die Folge sind Säumnisbeschwerden an das Bundesverwaltungsgericht. Hinzu kommt, dass mit vielen Entscheidungen „Neuland“ betreten wird und die zu entscheidenden Sachverhalte an inhaltlicher Komplexität zunehmen. Zusätzlich – wie in der Statistik ausgewiesen – haben viele Verfahren grenzüberschreitenden Charakter. Hier sind Partnerbehörden einzubinden und Übersetzungen vorzunehmen.

Neben der Führung von Verfahren besteht eine wesentliche Tätigkeit der DSB in der Mitwirkung auf europäischer Ebene, vor allem in den Untergruppen des Europäischen Datenschutzausschusses (EDSA). Diese Arbeitssitzungen finden teilweise im Monatsrhythmus statt.

Die Leiterin der DSB bekleidet seit 2018 die Funktion der Vorsitzenden des EDSA. Zur Unterstützung dieser Tätigkeit sind zwei Bedienstete der Datenschutzbehörde permanent eingebunden und stehen daher für sonstige Aufgaben der DSB nur eingeschränkt zur Verfügung.

Daneben war im Berichtszeitraum eine deutliche Zunahme an Vorabentscheidungsersuchen an den EuGH zu verzeichnen. Betrifft ein Vorabentscheidungsersuchen datenschutzrechtliche Fragen, wird die DSB im Rahmen des innerstaatlichen Entscheidungsprozesses, ob Österreich sich am Verfahren beteiligt, eingebunden. Die Erstellung von Schriftsätzen zu diesen Verfahren bindet ebenfalls Personalressourcen.

Eine Aufstockung des Personalstandes der DSB ist daher unausweichlich und dringend geboten, damit die DSB ihren gesetzlichen Aufträgen nachkommen kann.

5.1.2 Gliederung der DSB

Die im Jahr 2018 eingenommene Gliederung in 5 Büros, die im Datenschutzbericht 2018 beschrieben wurde, hat sich bewährt und ist unverändert.

Der Fokus aller Verfahren liegt auf den Büros 2 und 3, die die nationalen und grenzüberschreitenden Beschwerdeverfahren führen.

5.1.3 Verwaltungsstrafverfahren

Im Berichtszeitraum konnten zahlreiche Verwaltungsstrafverfahren abgeschlossen werden; es liegen auch erste Entscheidungen des BVwG vor.

Kennzeichnend für die Verwaltungsstrafverfahren sind die Tatsachen, dass sich ein Großteil gegen behauptete unzulässige Videoüberwachungen richtet (auch im Straßenverkehr mittels Dashcams) und dass beinahe jedes Straferkenntnis vor dem BVwG bekämpft wird.

Auch inhaltlich stellen die Verwaltungsstrafverfahren eine Herausforderung dar, weil die zentrale Strafnorm der DSGVO (Art. 83) etliche Fragestellungen aufwirft, die noch keiner (höchst-)gerichtlichen Entscheidung zugeführt wurden.

Die im Berichtszeitraum höchste verhängte Geldbuße betrug 18 Millionen Euro (nicht rechtskräftig).

5.1.4. Grenzüberschreitende Zusammenarbeit

Liegt ein grenzüberschreitender Sachverhalt vor, ist die DSB verpflichtet, andere Aufsichtsbehörden in das Verfahren einzubeziehen bzw. wird die DSB von diesen eingebunden.

Die grenzüberschreitende Zusammenarbeit verläuft zum überwiegenden Teil sehr gut. Als größte Herausforderung haben sich die unterschiedlichen nationalen Verfahrensbestimmungen herauskristallisiert. Während bspw. in Österreich das Recht auf Akteneinsicht integraler Bestandteil des behördlichen Verfahrens ist, ist dies in anderen Mitgliedstaaten nicht der Fall. Folglich müssen im Einzelfall seitens der DSB von der Partnerbehörde Unterlagen angefordert werden bzw. mit der Partnerbehörde abgestimmt werden, welche Aktenteile ggf. von der Akteneinsicht auszuschließen sind.

5.2 Verordnung über Überwachungsstellen zur Einhaltung von Verhaltensregeln gemäß Art. 41 DSGVO

Der Im Berichtszeitraum wurde der Entwurf einer Verordnung der Datenschutzbehörde über die Anforderungen an eine Stelle für die Überwachung der Einhaltung von Verhaltensregeln (Überwachungsstellenakkreditierungs-Verordnung – ÜStAkk-V) zur allgemeinen Begutachtung versendet und dem EDSA zur Stellungnahme nach Art. 64 DSGVO vorgelegt.

Die ÜStAkk-V wurde nach Abschluss dieses Prozesses im BGBl. II Nr. 264/2019 kundgemacht. Sie regelt, in Durchführung der Vorgaben des Art. 41 Abs. 2 DSGVO, die näheren Details hinsichtlich der Akkreditierung einer Überwachungsstelle.

Alle Verhaltensregeln nach Art. 40 DSGVO, die bei der DSB zur Genehmigung eingereicht werden, bedürfen einer unabhängigen Überwachungsstelle, die die Einhaltung der Verhaltensregeln überwacht.

Die DSGVO regelt zwar in Grundzügen die Anforderungen an eine Überwachungsstelle, überlässt aber den Aufsichtsbehörden die nähere Konkretisierung dieser Vorgaben. Damit diese Vorgaben unionsweit möglichst einheitlich erlassen werden, ist der EDSA im Vorfeld zu befassen.

Der Verordnungstext sowie die Erläuterungen dazu sind auf der Website der DSB abrufbar.

Die Stellungnahme des EDSA (Stellungnahme Nr. 9/2019) ist in englischer Sprache auf der Website des EDSA abrufbar.

5.3 Novelle des DSG im Jahr 2019 und weiterer Anpassungsbedarf

Das DSG wurde im Berichtszeitraum durch BGBl. I Nr. 14/2019 novelliert. Neben einer Bereinigung und Berichtigung von Redaktionsversehen ist die Aufhebung der Verfassungsbestimmungen der §§ 2 und 3 DSG hervorzuheben: Die Gesetzgebungs- und Vollzugskompetenz in allgemeinen Angelegenheiten des Schutzes personenbezogener Daten liegt nunmehr ausschließlich

beim Bund, die in § 2 DSG normierte Länderkompetenz (Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im nicht-automationsunterstützten Bereich) gibt es nicht mehr.

Eine Novelle des § 1 DSG (Grundrecht auf Datenschutz), welche im Zuge dieses Gesetzesvorhabens ebenfalls geplant war, kam aufgrund der fehlenden Mehrheit für eine Änderung dieser Verfassungsbestimmung nicht zustande.

Im Laufe des Jahres kam es zu einigen gerichtlichen Entscheidungen, die eine weitere Novelle des DSG erforderlich machen werden:

So hielt der **OGH** in seiner Entscheidung vom 23. Mai 2019, **6 Ob 91/19d**, fest, dass aus Art. 79 DSGVO ein unmittelbarer Zugang zu einem Zivilgericht abgeleitet werden kann. Das DSG regelt bis dato nur die gerichtliche Zuständigkeit für Schadenersatzklagen (§ 29 DSG). Die Zuständigkeit für (sonstige) zivilrechtliche Klagen auf Basis der DSGVO ist – anders als noch in § 32 DSG 2000 – nicht geregelt. Die genannte Entscheidung des OGH führt nunmehr dazu, dass ein Betroffener sich zur Geltendmachung datenschutzrechtlicher Ansprüche (mit Ausnahme des Schadenersatzes) wahlweise an die DSB (Beschwerde gemäß Art. 77 DSGVO iVm § 24 DSG) oder an ein Zivilgericht (Klage gemäß Art. 79 DSGVO) wenden kann. Um einander widersprechende Entscheidungen zu vermeiden, ist es daher erforderlich, im DSG flankierende Verfahrensbestimmungen vorzusehen (bspw. wechselseitige Aussetzungspflichten der DSB und der Zivilgerichte).

Das **BVwG** wiederum hat in zwei rezenten Entscheidungen die Gültigkeit von §§ 12 und 13 DSG (Bildverarbeitung) im Lichte der DSGVO in Zweifel gezogen und ausgesprochen, dass – in den konkreten Fällen – für § 13 DSG sowie § 12 Abs. 4 Z 1 DSG keine Öffnungsklausel besteht und diese Bestimmungen daher nicht anzuwenden sind (siehe dazu BVwG, Beschluss vom 20.11.2019, **W256 2214855-1**, und BVwG, Erkenntnis vom 25.11.2019, **W211 2210458-1**).

Diese Entscheidungen haben weitreichende Auswirkungen.

So wird die DSB, sofern im Einzelfall nicht besondere Gründe dafürsprechen, die §§ 12 und 13 DSG nicht mehr anwenden, sondern Bildverarbeitungen ausschließlich auf Basis der Art. 5 und 6 DSGVO prüfen. Dass eine Bildverarbeitung (in einem Mehrparteienhaus) auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden kann, hat der EuGH in einem rezenten Urteil (zur Rechtslage nach der Richtlinie 95/46/EG) bestätigt (EuGH, Urteil vom 11.12.2019, C-708/18). Eine Bildverarbeitung entspricht demgemäß nur dann der DSGVO, wenn sie zumindest auf einen Tatbestand gemäß Art. 6 Abs. 1 DSGVO (im Regelfall wird nur lit. f in Betracht kommen) gestützt werden kann und alle Vorgaben gemäß Art. 5 Abs. 1 DSGVO erfüllt sind. Dies wird im Rahmen einer Einzelfallbeurteilung zu prüfen sein.

6 Europäische Zusammenarbeit

6.1 Europäische Union

6.1.1 Der Europäische Datenschutzausschuss¹⁹

Der Europäische Datenschutzausschuss (EDSA) hat sich im Jahr 2019 monatlich (mit Ausnahme des Monats August) zu jeweils zweitägigen Plenarsitzungen getroffen.

Im Zuge dessen hat der EDSA gemäß Art. 64 Abs. 1 DSGVO zu folgenden Themen insgesamt 13 Stellungnahmen²⁰ abgegeben:

- 4 Stellungnahmen zu nationalen Listen (Lichtenstein, Norwegen, Spanien, Island und Zypern) über Verarbeitungstätigkeiten, die einer Datenschutz-Folgenabschätzung unterliegen;
- 3 Stellungnahmen zu nationalen Listen (Tschechien, Spanien und Frankreich) über Verarbeitungstätigkeiten, die keiner Datenschutz-Folgenabschätzung unterliegen;
- 2 Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (Equinix Inc. und ExxonMobil Corporation);
- 2 Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Überwachung von Verhaltensregeln gemäß Art. 41 DSGVO (Österreich, Vereinigtes Königreich);
- Eine Stellungnahme zum Entwurf der Standardvertragsklauseln gemäß Art. 28 Abs. 8 DSGVO (Dänemark).

Weiters hat der EDSA gemäß Art. 64 Abs. 2 DSGVO²¹ 2019 folgende Stellungnahmen²² angenommen:

- Eine Stellungnahme zum Entwurf einer Verwaltungsvereinbarung zwischen EWR- und Nicht-EWR-Finanzaufsichtsbehörden;
- Eine Stellungnahme zum Zusammenspiel zwischen der ePrivacy Richtlinie und der DSGVO, insbesondere hinsichtlich der Zuständigkeit, Aufgaben und Befugnisse der Datenschutzbehörden;
- Eine Stellungnahme zur Zuständigkeit einer Aufsichtsbehörde im Falle einer Änderung der Umstände in Bezug auf die Hauptniederlassung oder einzigen Niederlassung.

Zudem hat der EDSA 2019 zu folgenden Themen Leitlinien²³ angenommen:

- Verhaltensregeln und Überwachungsstellen (EDPB Guidelines 1/2019)
- Verarbeitung personenbezogener Daten nach Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten (EDPB Guidelines

19 Nähere Informationen zu den Aufgaben sowie zur Organisation des EDSA sind dem Datenschutzbericht 2018, Kapitel 6.1.1 zu entnehmen.

20 Die angeführten Stellungnahmen des EDSA sind unter folgendem Link abrufbar: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

21 Gemäß Art. 64 Abs. 2 DSGVO kann jede Aufsichtsbehörde, der Vorsitz des Datenschutzausschusses oder die Europäische Kommission, und gegebenenfalls die EFTA-Überwachungsbehörde beantragen, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedsstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten

22 Die angeführten Stellungnahmen des EDSA sind unter folgendem Link abrufbar: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

23 Diese Leitlinien des EDSA sind unter folgendem Link abrufbar: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

- 2/2019)
- Verarbeitung personenbezogener Daten durch Videoanlagen (EDPB Guidelines 3/2019)
- Data Protection by Design and by Default gemäß Art. 25 DSGVO (EDPB Guidelines 4/2019) [Version nach Abschluss des öffentlichen Konsultationsverfahrens, vor endgültiger Annahme durch den EDSA]
- Recht auf Vergessen werden in den Fällen betreffend Suchmaschinen (Teil 1) (EDPB Guidelines 5/2019)

Auch im Jahr 2019 wurden alle Expertenuntergruppen des EDSA seitens der DSB beschickt, jede Expertenuntergruppe traf sich dabei etwa alle zwei bis drei Monate zur Besprechung bzw. Vorbereitung der Arbeit des EDSA.

6.1.2 Europol

Das Europäische Polizeiamt (Europol) ist eine europäische Polizeibehörde mit der Aufgabe, die Leistungsfähigkeit der zuständigen Behörden der Mitgliedstaaten und ihre Zusammenarbeit im Hinblick auf die Verhütung und die Bekämpfung des Terrorismus, des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität zu verbessern. Europol verarbeitet zu diesem Zweck große Mengen von vor allem strafrechtsrelevanten Daten. Diese Verarbeitung unterlag bis Mai 2017 der besonderen Kontrolle durch eine gemeinsame Kontrollinstanz, die aus Vertretern aller EU Datenschutzbehörden bestand, dem „Europol Joint Supervisory Body“ (JSB). Mit der neuen Europol Verordnung²⁴ 794/2016 vom 11. Mai 2016, die am 01. Mai 2017 in Kraft trat, wurde diese gemeinsame Kontrollinstanz abgeschafft. An ihre Stelle trat eine aufgeteilte Kontrolle: Einerseits durch nationale Kontrollinstanzen, die die Zulässigkeit der Eingabe und des Abrufs personenbezogener Daten sowie jedweder Übermittlung dieser Daten an Europol überwachen und andererseits den Europäischen Datenschutzbeauftragten (EDSB), der die Verarbeitung durch Europol überwacht. Jede betroffene Person kann beim Europäischen Datenschutzbeauftragten eine Beschwerde einreichen, wenn sie der Ansicht ist, dass Europol bei der Verarbeitung ihrer personenbezogenen Daten gegen die Europol-Verordnung verstößt. Darüber hinaus kann jede Person die nationale Kontrollbehörde ersuchen, die Rechtmäßigkeit jeglicher Übermittlung ihrer personenbezogenen Daten an Europol sowie die Verarbeitung dieser Daten durch den betreffenden Mitgliedstaat zu prüfen. Die Vertreter der nationalen Kontrollbehörde der Mitgliedstaaten und der Europäische Datenschutzbeauftragte bilden gemeinsam den Beirat für Zusammenarbeit. Die Hauptaufgabe des Beirates ist es, sich mit den allgemeinen Richtlinien und Strategien von Europol im Bereich der Überwachung des Datenschutzes sowie der Zulässigkeit der Verarbeitung und die Übermittlung von personenbezogenen Daten an Europol auseinanderzusetzen.

6.1.3 Schengen

Das Schengener Informationssystem der zweiten Generation (kurz „SIS II“) ermöglicht nationalen Grenz-, Zoll-, Visa- und Strafverfolgungsbehörden Fahndungen zu gesuchten oder vermissten Personen bzw. gestohlenen oder verlorenen Sachen, insbesondere Dokumente und Fahrzeuge, im Schengen-Raum auszuschreiben bzw. abzufragen. Die Rechtsgrundlage für das SIS II bildet die sogenannte SIS-II-Verordnung.²⁵ Das SIS II besteht aus einem zentralen System (C.SIS), den jeweiligen nationalen Systemen der Mitgliedstaaten (N.SIS II) sowie einer Kommunikationsinfrastruktur zwischen dem zentralen System und den nationalen Systemen. Das österreichische N.SIS II wird vom Bundesministerium für Inneres als Verantwortlichem geführt. Die jeweiligen nationalen Datenschutzbehörden haben gemäß der SIS-II-Verordnung die Rechtmäßigkeit der Verarbeitung personenbezogener SIS-II-Daten auf nationaler Ebene zu überwachen. Darüber hinaus haben die nationalen Datenschutzbe-

24 <http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0794&from=EN>

25 <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32006R1987>

hörden mindestens alle vier Jahre die Datenverarbeitungsvorgänge im N. SIS II nach internationalen Prüfungsstandards zu überprüfen. Die Datenschutzbehörde hat diese Überprüfung im Jahr 2019 abgeschlossen.

Darüber hinaus überprüft die Europäische Kommission gemeinsam mit nationalen Experten die Umsetzung der SIS-II-Verordnung in den einzelnen Mitgliedsstaaten. Ein Mitarbeiter der Datenschutzbehörde hat als nationaler Experte an der Evaluierung in Polen mitgewirkt und wird im Jahr 2020 in diesem Zusammenhang auch Österreich überprüft werden.

6.1.4 Zoll

Das gemeinsame Zollinformationssystem (ZIS) dient der Erfassung von Daten von Waren, Transportmitteln, natürlichen und juristischen Personen, die im Zusammenhang mit Verstößen gegen das gemeinsame Zoll- und Agrarrecht stehen. Das ZIS ermöglicht einem Mitgliedstaat, der Daten in das System eingegeben hat, einen ZIS-Partner in einem anderen Mitgliedstaat um die Durchführung u.a. gezielter Kontrollen zu ersuchen. Zur Gewährleistung eines angemessenen Datenschutzes wurde neben dem Ausschuss gemäß Art. 43 der ZIS-Verordnung²⁶ („Joint Supervisory Authority of Customs“ („JSA“)) eine Koordinierende Aufsichtsbehörde (CIS Supervision Coordination Group („CIS-SCG“)) eingerichtet, welche aus Vertretern der nationalen Datenschutzbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten gebildet wird.

6.1.5 Eurodac

Das „Eurodac“-System ermöglicht den Einwanderungsbehörden der Mitgliedstaaten Asylwerber und andere Personen zu identifizieren, die beim illegalen Überschreiten einer EU-Außengrenze aufgegriffen werden. Anhand der Fingerabdrücke kann ein Mitgliedstaat feststellen, ob ein Fremder in einem anderen Mitgliedstaat Asyl beantragt hat oder ob ein Asylwerber illegal in die EU eingereist ist. Eurodac besteht aus einer von der Europäischen Kommission verwalteten Zentraleinheit und den in den Mitgliedsstaaten zur Abfrage und Befüllung betriebenen nationalen Systemen. Art. 32 der (EU) Verordnung Nr. 603/2013²⁷ sieht eine koordinierte Überwachung der nationalen Datenschutzbehörden mit dem Europäischen Datenschutzbeauftragten vor, wobei die Mitgliedstaaten jährlich eine Überprüfung der Verarbeitung personenbezogener Daten durchzuführen haben.

6.1.6 Visa

Das Visa-Informationssystem (VIS) enthält Daten zu Ausstellungen, Ablehnungen, Annullierungen, Widerrufen und Verlängerungen von Kurzzeit-Visa in den Mitgliedstaaten des Schengen Raums. Die rechtliche Grundlage für das VIS bildet die Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Einrichtung des Visa-Informationssystems (VIS-Verordnung). Das VIS besteht aus einem zentralen Visa-Informationssystem (CS-VIS), einem nationalen System (N-VIS) in jedem Mitgliedstaat und aus einer Kommunikationsinfrastruktur zwischen dem zentralen Visa-Informationssystem und den nationalen Systemen. In Österreich ist das Bundesministerium für Inneres Verantwortlicher des VIS. Die jeweiligen nationalen Datenschutzbehörden haben gemäß der VIS-Verordnung die Rechtmäßigkeit der Verarbeitung personenbezogener VIS-Daten auf nationaler Ebene zu überwachen. Darüber hinaus haben die nationalen Datenschutzbehörden mindestens alle vier Jahre die Datenverarbeitungsvorgänge im N-VIS nach internationalen Prüfungsstandards zu überprüfen. Die Datenschutzbehörde hat eine entsprechende Überprüfung im Jahr 2019 begonnen.

26 <http://eur-lex.europa.eu/legal-content/de/TXT/?uri=celex:31997R0515>

27 <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32013R0603>

6.2 Europarat

Die Datenschutzbehörde vertritt die Republik Österreich im Ausschuss nach Art. 18 (T-PD) der Datenschutzkonvention des Europarates (EVS Nr. 108; BGBl. Nr. 317/1988). Im Berichtszeitraum fanden von 13. bis 14. Juni 2019 die 38. Plenarsitzung und von 19. bis 21. November 2019 die 39. Plenarsitzung des T-PD in Straßburg statt. Die Tagesordnungen sowie die zusammenfassenden Berichte der Sitzungen sind in englischer Sprache unter <https://www.coe.int/en/web/data-protection/consultative-committee-tpd/meetings> abrufbar.

7 Internationale Beziehungen

EU-U.S. Privacy Shield – 3rd Annual Joint Review

Gemäß des am 12. Juli 2016 angenommenen EU-US-Datenschutzschildes („EU-U.S. Privacy Shield“) nahmen acht Vertreter des Europäischen Datenschutzausschusses (EDSA), darunter auch eine Vertreterin der österreichischen Datenschutzbehörde, am 12. und 13. September 2019 an der dritten gemeinsamen Überprüfung der Angemessenheitsentscheidung durch die Europäische Kommission in Washington, D.C. teil. Diese jährlichen Überprüfungen dienen dazu, die Robustheit der Angemessenheitsentscheidung und ihre praktische Umsetzung zu bewerten.

Ausgehend von vorangegangenen Stellungnahmen der Art. 29 Datenschutzgruppe und des EDSA, insbesondere der Stellungnahme 01/2016 sowie den Berichten zu den zwei bisherigen gemeinsamen Überprüfungen der Vorjahre, konzentrierte sich der EDSA auf die Bewertung der kommerziellen Aspekte des Privacy Shields und auch des Zuganges der amerikanischen Regierung zu personenbezogenen Daten, die aus der Europäischen Union zum Zwecke der Strafverfolgung und der nationalen Sicherheit übermittelt werden, einschließlich der den EU-Bürgern zur Verfügung stehenden Rechtsbehelfe. Hierbei prüfte der EDSA insbesondere, ob die bisher geäußerten Bedenken ausgeräumt wurden und, ob die im Rahmen des EU-U.S. Privacy Shields gewährten Garantien praktikabel und wirksam sind.

Die wichtigsten Ergebnisse dieser dritten Überprüfung, die sich sowohl aus schriftlichen Eingaben, als auch aus mündlichen Beiträgen ergeben, wurden im Bericht²⁸ des EDSA präzise dargestellt. Überdies veröffentlichte die Europäische Kommission einen eigenständigen Bericht²⁹ am 23. Oktober 2019.

Den Schlussfolgerungen des EDSA-Berichtes ist im Wesentlichen zu entnehmen, dass die Bemühungen der US-Behörden und der Europäischen Kommission zur Umsetzung des Privacy Shields, insbesondere die von Amts wegen durchgeführten Aufsichts- und Durchsetzungsmaßnahmen sowie die Ernennung der letzten fehlenden Mitglieder des „Privacy and Civil Liberties Oversight Board“ (PCLOB) und einer permanenten Ombudsperson begrüßt werden. Dennoch hat der EDSA nach wie vor eine Reihe von Bedenken, die sowohl von der Europäischen Kommission als auch von den US-Behörden ausgeräumt werden müssen.

Im Hinblick auf die kommerziellen Aspekte des Privacy Shields äußerte der EDSA weiterhin Bedenken über das Fehlen substantieller Kontrollen. Zudem bedürfen die Umsetzung der Anforderungen

28 https://edpb.europa.eu/our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-report-12112019_en

29 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

des Privacy Shields, in Bezug auf Weiterübermittlungen und Personaldaten, sowie die Anwendung der Grundsätze, in Bezug auf Auftragsverarbeiter und das Rezertifizierungsverfahren, weitere Aufmerksamkeit. Ein umfangreicherer Zugang der Mitglieder des EDSA-Überprüfungsteams zu nicht öffentlichen Informationen, die kommerzielle Aspekte und laufende Untersuchungen betreffen, wäre überdies für die jährlichen Überprüfungen von Vorteil.

Was die Datenerhebungen durch die amerikanischen Behörden anbelangt, so kann der EDSA das PCLOB nur ermutigen, weitere Berichte zu erarbeiten und zu publizieren. Insbesondere wäre etwa ein weiterer Bericht zur Presidential Policy Directive 28 (PPD-28) wünschenswert. Der EDSA bedauert in diesem Kontext auch, dass zu Abschnitt 702 FISA kein allgemeiner Bericht des PCLOB vorgesehen ist sowie, dass Berichte über den Erlass 12333 höchstwahrscheinlich unter Verschluss bleiben. Hierzu betont der EDSA, dass Mitglieder des EDSA-Überprüfungsteams nur Zugang zu jenen Dokumenten erhalten, die auch der Öffentlichkeit zur Verfügung stehen. Der Zugang zu solchen Dokumenten wäre jedoch auch hier sinnvoll, um aussagekräftigere Überprüfungen zu ermöglichen.

Was den Ombudsperson-Mechanismus betrifft, so wurden während der diesjährigen Überprüfung einige neue Elemente vorgelegt, welche insbesondere auch die verfahrenstechnischen Aspekte des ersten Falles unter dem Ombudsperson-Mechanismus betrafen, der letztendlich für unzulässig erklärt wurde. Der EDSA ist jedoch trotz aller Verbesserungen noch immer nicht zu dem Schluss gekommen, dass die Ombudsperson über ausreichende Befugnisse für den Zugang zu Informationen und für die Behebung von Verstößen verfügt. Daher kann der EDSA auch nach wie vor nicht feststellen, dass die Ombudsperson als wirksamer Rechtsbehelf vor einem Gericht im Sinne von Art. 47 der EU-Grundrechtecharta angesehen werden kann.

Nachruf auf Hofrat Mag. Georg Lechner und Mag. Samraa El Fohail

HR Mag. Georg Lechner

Die Bediensteten der Datenschutzbehörde haben mit großer Trauer und Bestürzung erfahren, dass unser allseits geschätzter und geachteter Kollege Mag. Georg Lechner am 16. April 2019 verstorben ist.

Georg war für uns alle ein Eckpfeiler der Datenschutzbehörde und vor allem des Datenschutzes. De facto seit es die Datenschutzkommission (als Vorgängerin der Datenschutzbehörde) gab, gehörte ihr Georg an. Er hat somit alle wesentlichen Entwicklungen der vergangenen Jahrzehnte erlebt und vor allem mitgeprägt:

Die Geschäftsstelle der ehemaligen Datenschutzkommission und die Datenschutzabteilung des Bundeskanzleramtes (zuständig für die Legistik des Datenschutzgesetzes) waren über lange Jahre in Personalunion verbunden. Als die Geschäftsabteilung der Datenschutzkommission als eigene Abteilung des Bundeskanzleramtes-Verfassungsdienst etabliert wurde, wechselte Georg in diese. In diese Zeit fielen auch die formelle „Herauslösung“ der Geschäftsstelle aus dem Organisationsbereich des Bundeskanzleramtes im Mai 2013 infolge eines EuGH-Urteils und die Überleitung der Datenschutzkommission in die Datenschutzbehörde Ende 2013/Anfang 2014.

Georg hat in all diesen Zeiten der Datenschutzkommission/der Datenschutzbehörde die Treue gehalten und sein umfassendes Wissen tagtäglich eingebracht. Er war die einzige Person der ehemaligen Datenschutzkommission, die ALLE Verfahren nach dem DSG 2000 abdecken konnte: So war Georg nicht nur für das Datenverarbeitungsregister tätig, sondern führte auch Beschwerdeverfahren, Kon-

troll- und Ombudsmannverfahren sowie Verfahren betreffend internationalen Datenverkehr (IDVK). Daneben vertrat er die Datenschutzbehörde auf europäischer Ebene in der „Technology Subgroup“.

Sein Hauptinteresse und seine berufliche Leidenschaft galt aber dem internationalen Datenverkehr: Georg hat sich mit Akribie in diese komplexe Materie eingearbeitet und in jedes noch so undurchsichtige Konzerngeflecht Licht gebracht. Er hat mit Langmut und Ausdauer den Antragstellern Klarstellungen abgerungen und sie von der Richtigkeit seiner Rechtsauffassung überzeugt. Es kann getrost gesagt werden, dass seine Rechtsauffassung in diesem Bereich mit der Rechtsauffassung der Datenschutzbehörde gleichzusetzen war. Sein enormes Fachwissen war nicht nur innerhalb der Behörde, sondern auch bei den Antragstellern geschätzt.

Ein weiteres Interesse galt technologischen Neuerungen. Obwohl nicht der Generation der „digital natives“ angehörend, hat Georg der rasanten Entwicklung im digitalen Bereich großes Interesse entgegengebracht und konnte sein erworbenes Wissen zum Gewinn der Datenschutzbehörde in die Technology Subgroup auf europäischer Ebene einbringen.

Georg hat in seiner Person all das verkörpert, wofür die Datenschutzbehörde steht: Umfassendes Wissen im Bereich des rechtlichen und technischen Datenschutzes, Zusammenarbeit im internationalen und europäischen Bereich, Unvoreingenommenheit bei der Behandlung von Geschäftsfällen und konsequentes Vertreten der eigenen Position nach außen.

Neben seinem Fachwissen werden wir Georg auch als Mensch vermissen. Er hat zahlreiche Kolleginnen und Kollegen, die in die Datenschutzkommission kamen, eingeschult und mit allen Facetten der Verfahren vertraut gemacht. Uns allen hat Georg mit seiner väterlichen und fürsorglichen Art den Einstieg erleichtert: Er stand nicht nur am Anfang mit Rat und Tat zur Seite, sondern war auch später für Fragen und Diskussionen offen.

Wir vermissen Georg schmerzlich. Ehre seinem Andenken, möge er in Frieden ruhen.

Mag. Samraa El Fohail

Mit großer Trauer müssen wir bekannt geben, dass unsere liebe und allseits geschätzte Kollegin Mag^a. Samraa El Fohail am 28. Dezember 2019 völlig überraschend verstorben ist.

Mag^a. El Fohail ist im Zuge des In-Geltung-Tretens der Datenschutz-Grundverordnung im Mai 2018 vom Bundesministerium für Verkehr, Innovation und Technologie zur Datenschutzbehörde gewechselt. Sie hat sowohl im Büro 1 (Präsidialangelegenheiten/Legistik) als auch im Büro 5 (Verwaltungsstrafsachen) gearbeitet und konnte dort ihre unbestrittene Expertise einbringen. So war sie unter anderem für die Ausarbeitung der Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) und die Verordnung über die Anforderungen an eine Stelle für die Überwachung der Einhaltung von Verhaltensregeln (Überwachungsstellenakkreditierungs-Verordnung (ÜStAkk-V) maßgeblich verantwortlich. Mag^a. El Fohail hat darüber hinaus etliche Verwaltungsstrafverfahren geführt und dabei stets ein gerechtes und verhältnismäßiges Augenmaß bei der Beurteilung des jeweiligen Sachverhaltes bewiesen.

Durch ihr Ableben verliert die Datenschutzbehörde nicht nur eine äußerst fachkundige, engagierte und hilfsbereite Mitarbeiterin, sondern auch einen hochgeschätzten Menschen.

Wir werden Samraa schmerzlich vermissen. Mögest Du in Frieden ruhen!