Datenschutzbericht 2020

Wien, im März 2021

Impressum

Medieninhaber, Herausgeber und Redaktion:
Datenschutzbehörde, Dr. Andrea Jelinek
(gemäß § 18ff DSG), 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, 2021

Inhalt

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 (black list/white list) 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 2020 – wie von allen Menschen - geprägt von der Pandemie, damit einhergehenden Fragestellungen, die unmittelbar zu beantworten waren, sowie dem Bemühen aller Mitarbeiterinnen und Mitarbeiter die Funktionsfähigkeit der Behörde zu gewährleisten. So wurden beispielsweise beginnend mit März 2020 FAQs datenschutzrechtlicher Natur die Pandemie betreffend auf die Website der Behörde gestellt, die laufend ergänzt wurden und werden. Ich möchte mich an dieser Stelle bei all meinen Mitarbeiterinnen und Mitarbeitern für die großartige Zusammenarbeit und die hervorragende Arbeitsdisziplin im Berichtszeitraum bedanken. Ohne ihre kreativen Ideen, technischen Kenntnisse, Fleiß und Engagement wäre es nicht möglich gewesen, die Arbeit in diesem schwierigen Jahr 2020 so zu gestalten, dass auf die Herausforderungen entsprechend geantwortet werden konnte. Es wurden tausende nationale Verfahren geführt und abgeschlossen, im internationalen Bereich tatkräftig mitgearbeitet und der Gesundheitskrise persönlich und fachlich entgegengehalten.

Darüber hinaus haben die Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörde im Jahr 2020 sowohl national als auch international unzählige – in den meisten Fällen im Videomodus - Vorträge gehalten, (virtuelle) Veranstaltungen und Konferenzen im Bereich des Datenschutzes besucht. Trotz der erschwerten Bedingungen ist es gelungen – gemeinsam mit der Universität Wien – ein EU-Projekt zu beantragen und den Zuschlag hiefür zu erhalten.

Die Aufgabe der europäischen Datenschutzbehörden, die einheitliche Anwendung der Verordnung in der europäischen Union zu gewährleisten, wurde durch die Pandemie nicht erleichtert. Eine noch engere Zusammenarbeit der europäischen Datenschutzbehörden und eine Vervielfachung der Sitzungen des Europäischen Datenschutzausschusses haben auch in diesem Bereich zu wesentlichen Leitlinien und Entscheidungen des Ausschusses die datenschutzrechtlichen Herausforderungen der Pandemie betreffend geführt.

Der Datenschutzbericht 2020 ist der siebente, 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 – durchaus auch für Nicht-Juristinnen und Nicht-Juristen – konzipierten Leitfaden zur DSGVO auf ihrer Website zur Verfügung, der regelmäßig aktualisiert wird. Die jüngste Aktualisierung erfolgte im Jänner 2021

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 Adressdaten 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

An dieser Stelle sei festgehalten, dass die Datenschutzbehörde im Jahr 2020 und für das Jahr 2021 insgesamt 11 zusätzliche A1 Planstellen (höherer Dienst), sowie 2 A2 Planstellen (gehobener Dienst) erhalten hat. Die Anzahl von nunmehr 45,9 Vollzeitäquivalenten wird hoffentlich der Vielzahl an Beschwerden und der zusätzlichen Tätigkeiten, die die Behörde seit 25.Mai 2018 wahrzunehmen hat, ab nun gerecht werden können. An dieser Stelle möchte ich Frau Bundesministerin Dr. Alma Zadic und ihrem Team für ihren persönlichen und unermüdlichen Einsatz für die Personalerhöhung der österreichischen Datenschutzbehörde danken.

Im Berichtszeitraum versahen am Jahresende 2020 47 Personen in Teil- oder Vollzeit ihren Dienst bei der Datenschutzbehörde, davon 32 Juristinnen und Juristen (davon fünf Praktikanten), 4 Mitarbeiterinnen und 1 Mitarbeiter im gehobenen Dienst und 10 Mitarbeiterinnen und Mitarbeiter im Fachdienst. Die Bediensteten der Datenschutzbehörde sind in Erfüllung ihrer Aufgaben an die Weisungen der Leitung gebunden.

Die Vielzahl der Beschwerden führte nicht nur zu einer sehr hohen Arbeitsbelastung, die Verfahrensführung dieser nationalen und internationalen Beschwerden bedingt auch großes Fachwissen. Flexibles switchen zwischen Deutsch und Englisch als Arbeitssprachen ist erforderlich.

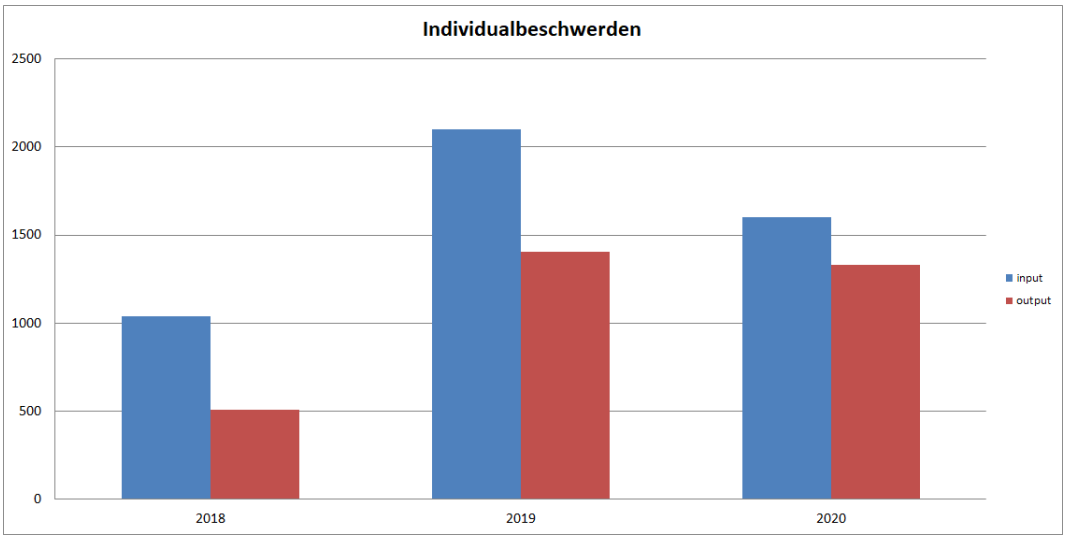
3 Tätigkeit der Datenschutzbehörde

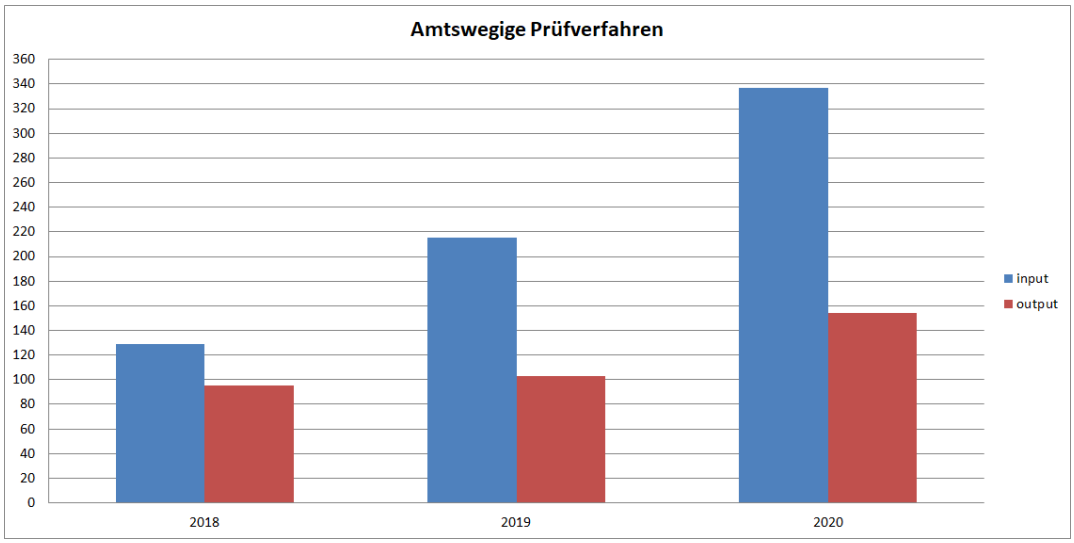
3.1 Statistische Darstellung

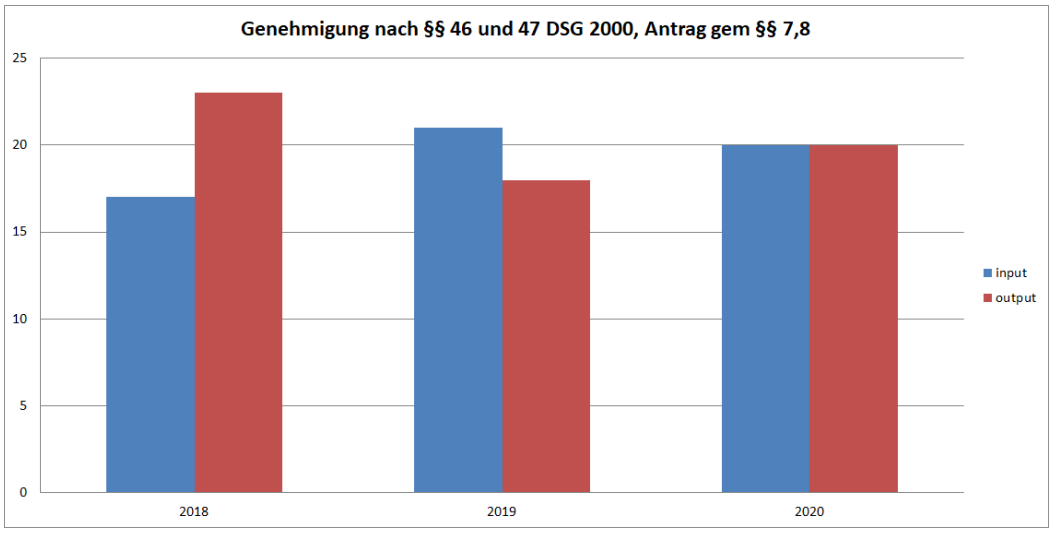
Tabelle 1 Anzahl der Eingangsstücke und Erledigungen

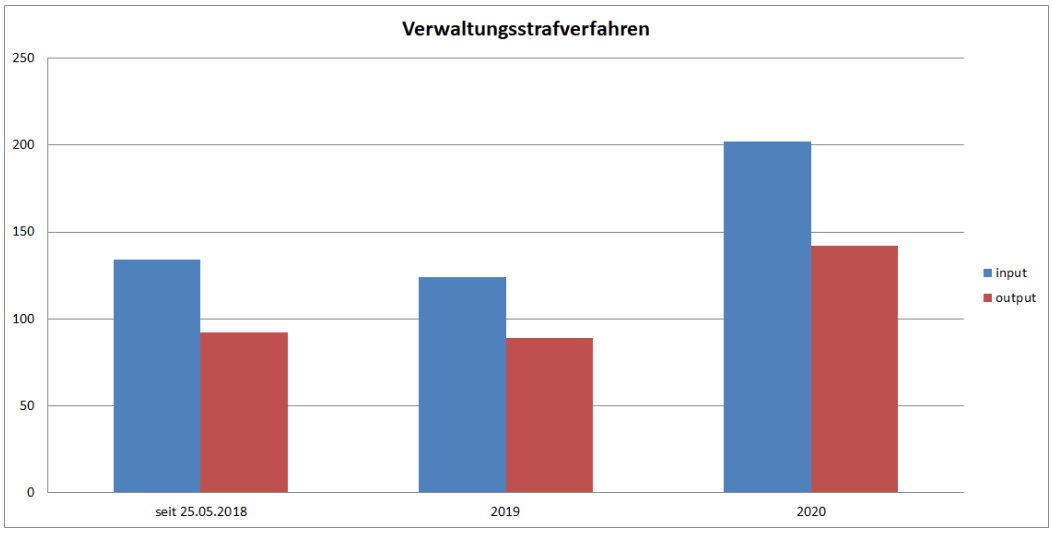
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2018	2019	2020	2018	2019	2020
Individualbeschwerden	1036	2102	1603	509	1405	1332
Erledigungsart der Individualbeschwerden				340 Bescheide 169 Einstellungen	828 Bescheide 577 Einstellungen	852 Bescheide 480 Einstellungen
Beschwerden Grenzüberschreitend seit 25.05.2018 (im Ausland einlangend	430	698	474	200	407	403
Beschwerden Grenzüberschreitend seit 25.05.2018 (in Österreich einlangend)	153	177	219	53	88	109
Amtswegige Prüfverfahren	129	215	337	95	103	154
Genehmigungen nach §§ 46 und 47 DSG 2000 (wissenschaftliche Forschung u. Statistik) Antrag gem. §§ 7,8	17	21	20	23	18	20
Genehmigungen im Internationalen Datenverkehr	27	1	0	119	1	0
Auskunft Schengen	19	114	127	16	104	127
Verwaltungsstrafverfahren seit 25.05.2018	134	124	202	92	89	142
Standardvertragsklauseln seit 25.05.2018	1	2	0	0	1	1
Verfahren vor dem Bundesverwaltungsgericht	50	164	319			

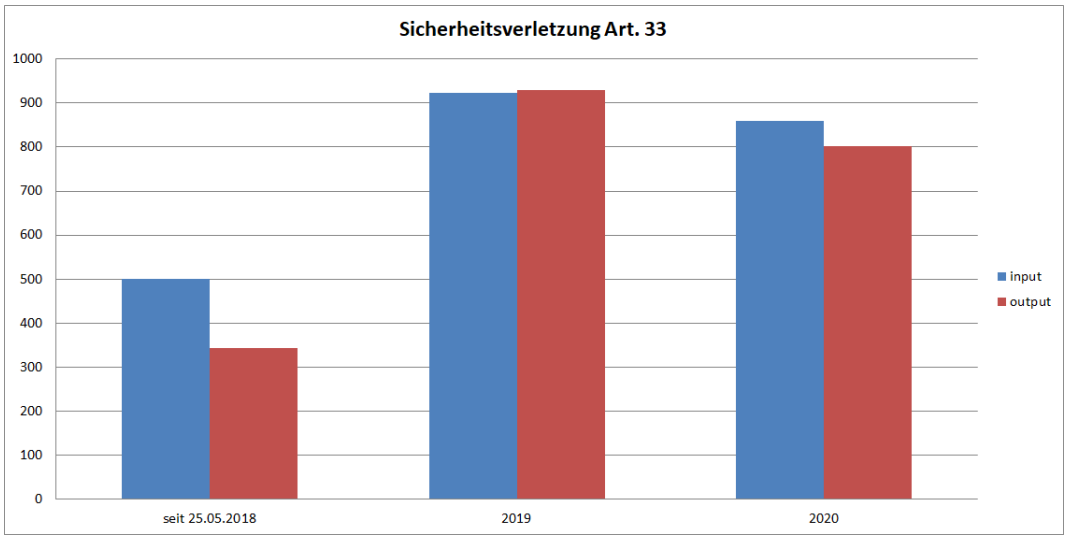
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2018	2019	2020	2018	2019	2020
Sicherheitsverletzungen § 95a	69	44	60	77	44	61
Sicherheitsverletzungen Art 33 seit 25.05.2018	501	923	860	344	929	802
Sicherheitsverletzungen grenz-überschreitend seit 25.05.2018 (in Österreich eingelangend	7	11	14	4	14	10
Sicherheitsverletzungen grenz-überschreitend seit 25.05.2018 (im Ausland einlangend)	43	71	76	8	41	45
Rechtsauskünfte	4052	4384	3166	3974	4329	3227
Amtshilfeersuchen Ausland	13	40	59	5	33	47
Anträge auf Genehmigung von Verhaltensregeln seit 25.05.2018	8	6	2	1	8	2
Genehmigung BCR (International)	60	20	5	60	20	2
Konsultationsverfahren seit 25.05.2018	2	5	1	2	3	1
Datenschutzbeauftragte	4754	922	632	4754	922	632
Verkehr mit Behörden	226	163	140	226	163	140

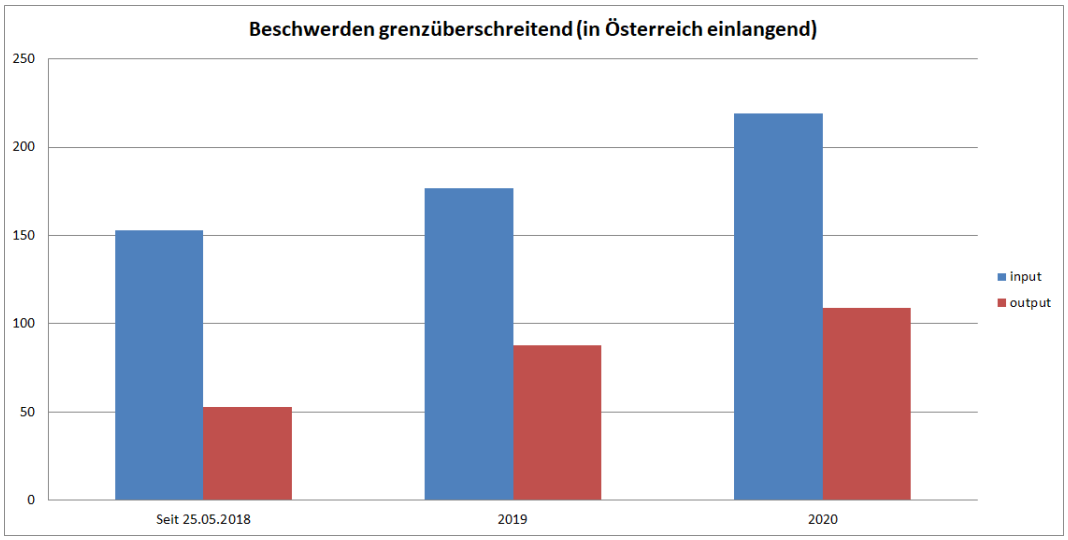


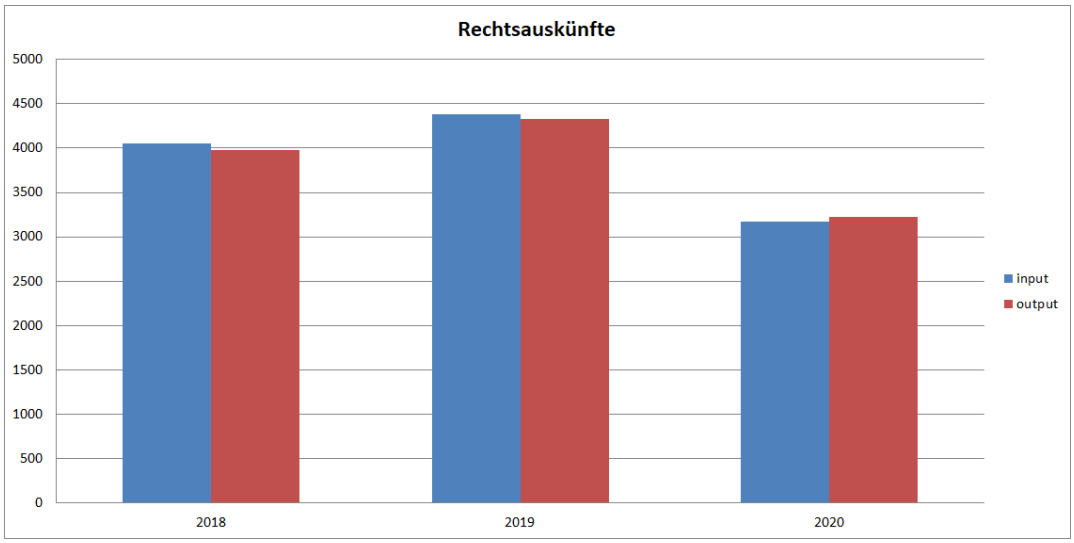

Amtswegige Prüfverfahren
360
340
320
300
280
260
240
220
200
180
160
140
120
100
80
60
40
20
0
2018
2019
2020
input
output

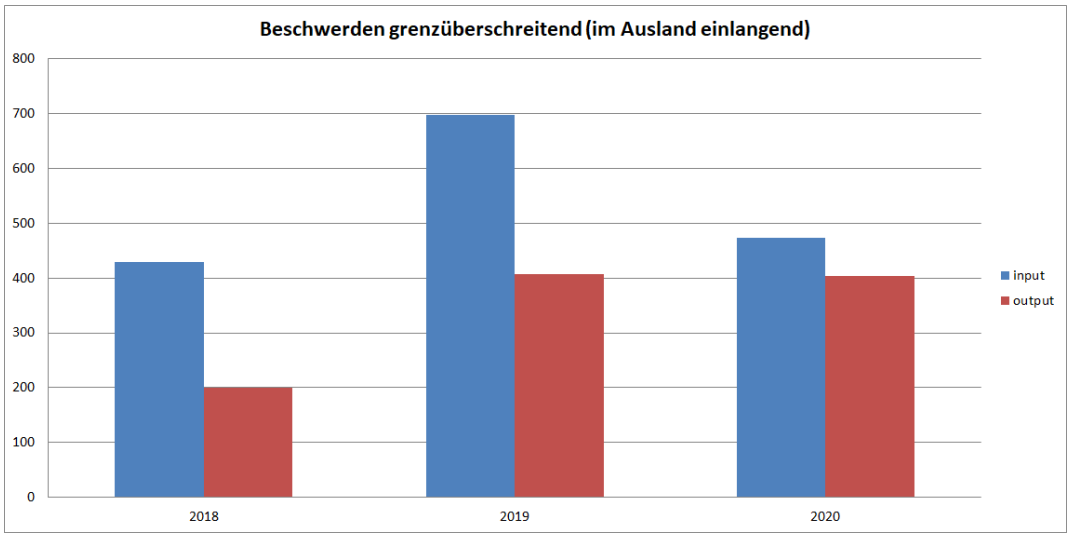

Genehmigung nach §§ 46 und 47 DSG 2000, Antrag gem §§ 7,8
25
20
15
10
5
0
2018
2019
2020
input
output


Verwaltungsstrafverfahren
250
200
150
100
50
0
seit 25.05.2018
2019
2020
input
output


Sicherheitsverletzung Art. 33
1000
900
800
700
600
500
400
300
200
100
0
seit 25.05.2018
2019
2020
input
output


Beschwerden grenzüberschreitend (in Österreich einlangend)
250
200
150
100
50
0
Seit 25.05.2018
2019
2020
input
output


Rechtsauskünfte
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
2018
2019
2020
input
output



3.2 Verfahren und Auskünfte

3.2.1.1 Individualbeschwerden Inland

Allgemeines und Grundsätzliches

Das Beschwerdeverfahren nach § 24 DSG 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 DSG 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 Inhaltser-

fordernisse des § 24 Abs. 2 und 3 DSG 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 Barrierefreiheit 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 Prüforganen wie Rechnungshof und Volksanwaltschaft)[1],
- 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 das Bundesverwaltungsgericht 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 einzubrin-

1 Hinweis: Das BVwG hat mit Erkenntnis vom 23.11.2020, GZ W211 2227144-1, eine Zuständigkeit der DSB gegenüber Organen der Gesetzgebung bejaht. Die DSB hat dagegen Amtsrevision an den VwGH erhoben, das Verfahren ist anhängig.

gen (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 2020

Im Berichtsjahr 2020 wurden insgesamt 1603 Individualbeschwerden bei der Datenschutzbehörde eingebracht. Im Vergleich zum „Rekord"-Jahr 2019 mit der bislang höchsten Anzahl von insgesamt 2102 Individualbeschwerden bedeutet dies einen Rückgang um etwa 24 %. Wie insgesamt seit Wirksamwerden der DSGVO am 25.05.2018, ist die Zahl der Individualbeschwerden auch im Berichtsjahr 2020 weiterhin beachtlich groß. Weitere Details enthält das Kapitel Statistik (Abschnitt 3.1).

Auch 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) waren im Berichtszeitraum kein Gegenstand berichtenswerter Entscheidungen.

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 mehrfach von der Möglichkeit Gebrauch gemacht, die Behandlung von Beschwerden gemäß Art. 57 Abs. 4 DSGVO wegen exzessiver Nutzung des Beschwerderechts abzulehnen.

Ausgewählte Beschwerdeentscheidungen aus 2020

Die DSB hat in ihrer öffentlich zugänglichen Entscheidungsdokumentation (im Rahmen des Rechtsinformationssystems des Bundes – RIS; Stand: 25.01.2021) aus dem Jahr 2020 9 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 2020 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.

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

Die wichtigsten Entscheidungen in chronologischer Reihenfolge:

1. **Bescheid vom 03.01.2020, GZ: DSB-D124.1090/0005-DSB/2019 (Verletzung im Recht auf Geheimhaltung: Führerschein und Bankomatkarte fotografiert und auf WhatsApp versendet)**

Hier hatte sich die Datenschutzbehörde mit der Verarbeitung personenbezogener Daten im Zusammenhang mit einer nicht bezahlten Beförderungsdienstleistung auseinanderzusetzen. Der Beschwerdeführer hatte eine Beförderungsdienstleistung des Beschwerdegegners, der ein Taxi-Unternehmen betreibt, in Anspruch genommen. Da der Beschwerdeführer nicht über genügend Bargeld verfügte, um bezahlen zu können, fertigte der Beschwerdegegner ohne Einwilligung des Beschwerdeführers ein Foto von dessen Führerschein und Bankomatkarte an, wobei er das Führerschein-Foto per „Whatsapp" an zumindest eine dritte Person (einen Bekannten des Beschwerdegegners) weiterleitete.

Die Datenschutzbehörde gab der Beschwerde statt und stellte eine Verletzung im Recht auf Geheimhaltung des Beschwerdeführers fest, da weder die Datenerhebung (Fotografieren) noch die Datenübermittlung (Weiterleiten per Whatsapp) rechtmäßig war. Der Beschwerdegegner konnte sich diesbezüglich weder auf ein lebenswichtiges Interesse des Betroffenen noch dessen Zustimmung stützen. Eine Verarbeitung im überwiegenden berechtigten Interesse des Beschwerdegegners war ebenfalls zu verneinen, da das Foto¬grafieren des Führerscheins und der Bankomatkarte sowie das Weiterleiten des Führerschein-Fotos an einen Bekannten des Beschwerdegegners unverhältnismäßig war und gegen den Grundsatz der Datenminimierung iSd. Art. 5 Abs. 1 lit. c DSGVO verstieß.

Dieser Bescheid ist nicht rechtskräftig.

2. **Bescheid vom 16.01.2020, GZ: DSB-D123.815/0002-DSB/2019(Patientenbogen frei zugänglich mit Diagnose/Medikation)**

Die Datenschutzbehörde hatte sich hier mit einer Beschwerde im Recht auf Geheimhaltung (§ 1 DSG) auseinander zu setzen.

Der Beschwerdeführer wurde von seinem Arbeitgeber zu einer periodischen Untersuchung bei der Beschwerdegegnerin, einem Arbeitsmedizinischen Zentrum, geladen. Vor der Untersuchung hat der Beschwerdeführer ein Patientenblatt ausgefüllt und Angaben zu seinem Gesundheitszustand und seinen Medikamenten gemacht. Einige Tage später wurde der Beschwerdeführer von einem ehemaligen Arbeitskollegen kontaktiert (der selbst zu einer Untersuchung bei der Beschwerdegegnerin geladen war) und darauf aufmerksam gemacht, dass der Patientenbogen des Beschwerdeführers offen herumliegen würde. Der ehemalige Kollege konnte namentlich die Medikamente sowie die Wohnadresse des Beschwerdeführers nennen.

Im gegenständlichen Fall war es so, dass eine Mitarbeiterin der Beschwerdegegnerin die Unterlagen des Beschwerdeführers auf ihrem Schreibtisch abgelegt hatte. Im Zuge einer kurzfristen Abwesenheit der Mitarbeiterin war es dem ehemaligen Arbeitskollegen möglich, Einsicht zu nehmen. Wie genau es diesem gelang, Einsicht in die Unterlagen zu nehmen und ob – wie von der Beschwerdegegnerin vorgebracht, eine bewusste und absichtliche Handlung dazu führte – konnte im Ermittlungsverfahren nicht mehr festgestellt werden. Festgestellt werden konnte aber, dass die Mitarbeiterin der Beschwerdegegnerin sensible Unterlagen des Beschwerdeführers in unmittelbarer Nähe von Dritten offen abgelegt hatte.

Rechtlich ergab sich daher, dass die Beschwerdegegnerin den Beschwerdeführer im Recht auf Geheimhaltung verletzt hatte, indem Unterlagen, die Angaben zum Gesundheitszustand und Medikamen-tengebrauch des Beschwerdeführers enthielten, offen liegen gelassen wurden, womit es einem Dritten möglich war, Einsicht in selbige zu nehmen.

Dieser Bescheid ist rechtskräftig.

3. Bescheid vom 10.02.2020, GZ: 2020-0.046.690(Amtshilfe nach Art. 22 B-VG als geeignete Rechtsgrundlage iSd § 38 DSG)

Der Beschwerdeführer erachtete sich durch eine Staatsanwaltschaft (im Folgenden: StA) im Recht auf Geheimhaltung als verletzt. Diese hatte aufgrund eines Amtshilfeersuchens ein psychiatrisches Gutachten zum Beschwerdeführer an die ersuchende Landepolizeidirektion (im Folgenden: LPD) weitergegeben. Die LPD hatte nämlich über einen Antrag des Beschwerdeführers auf Löschung seiner erkennungsdienstlichen Daten zu entscheiden und deshalb Informationen über diesen bei der StA angefordert. Die StA wiederum hatte zuvor gegen den Beschwerdeführer wegen Anstiftung zum Amtsmissbrauch wie auch wegen gefährlicher Drohung ermittelt, wobei das Strafverfahren wegen Zurechnungsunfähigkeit eingestellt worden war.

Die Datenschutzbehörde verwies zunächst darauf, dass auf den Fall das 3. Hauptstück des DSG anzuwenden ist, mit dem die DSRL-PJ umgesetzt wurde. Art. 8 DSRL-PJ, der in § 43 DSG umgesetzt wurde, legt fest, dass eine Verarbeitung zu Zwecken der DSRL-PJ nur dann rechtmäßig ist, wenn sie gesetzlich vorgesehen ist.

Die Datenschutzbehörde entschied, dass sowohl die Beschwerdegegnerin die Daten – hier: das psychiatrische Gutachten – im Zuge des Strafverfahrens gesetzlich erhoben und auch die LPD zur Behandlung des Löschungsantrages nach SPG ermächtigt war, das psychiatrische Gutachten für eine Gefährdungsprognose des Beschwerdeführers zu verwenden.

Die Datenschutzbehörde führte weiter aus, dass Art. 22 B-VG, der die Amtshilfe statuiert, eine geeignete Rechtsgrundlage darstellt, um sensible Daten zu übermitteln. Im vorliegenden Fall hatte sich die LPD in ihrem Amtshilfeersuchen auf § 76 StPO, der ebenfalls die Amtshilfe regelt, gestützt. § 76 StPO präzisiert den Art. 22 B-VG nur näher. Die Übermittlung des Gutachtens von der Beschwerdegegnerin an die LPD war daher rechtmäßig.

Der Bescheid ist nicht rechtskräftig.

4. Bescheid vom 11.02.2020, GZ: DSB-D124.024/0008-DSB/2019(Speicherdauer von Stammdaten iSd § 97 TKG 2003 durch einen Mobilfunkanbieter)

Die Datenschutzbehörde beschäftigte sich mit der Frage, wie lange ein Mobilfunkanbieter nach Beendigung eines Vertrages Stammdaten aufbewahren darf. Bei Stammdaten handelt es sich um Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind (zB Name, Anschrift, Information über Art und Inhalt des Vertragsverhältnisses). Der Mobilfunkanbieter verweigerte zum Teil die beantragte Löschung und brachte vor, Stammdaten würden erst nach sieben Jahren ab Vertragsbeendigung gelöscht werden. Grundlage dafür seien die Bestimmungen § 132 BAO sowie § 212 UGB.

Dazu führte die Datenschutzbehörde aus, dass § 97 Abs. 1 TKG 2003 eine strenge Zweckbindung für die Verarbeitung personenbezogener Daten normiert. Gemäß § 97 Abs. 2 TKG 2003 sind Stammdaten spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen. § 132 BAO und § 212 UGB normieren zwar eine Aufbewahrungspflicht von sieben Jahren und stellen daher auch grundsätzlich eine Rechtsgrundlage für die weitere Verarbeitung der Daten nach Vertragsbeendigung dar. Die siebenjährige Frist beginnt jedoch nicht ab Beendigung des Vertrages zu laufen, sondern gemäß ausdrücklichem Gesetzeswortlaut dieser Bestimmungen bereits ab Schluss des Geschäftsjahres, auf das sich die Unterlagen beziehen.

Dieser Bescheid ist rechtskräftig.

5. Bescheid vom 20.02.2020, GZ: 2020-0.059.515(Datenweitergabe von Mieterdaten von der Hausverwaltung an einen Subdienstleister gesetzlich gedeckt)

Hier hatte sich die Datenschutzbehörde mit der Datenweitergabe von Namens- und Telefondaten eines Mieters von der Hausverwaltung an einen Subdienstleister zur Konfliktlösung zu befassen.

Der Beschwerdeführer setzte zunächst die Hausverwaltung telefonisch vom ungebührlichen Verhalten eines Mieters in Kenntnis. Eine Mitarbeiterin der Hausverwaltung nahm den Sachverhalt auf und informierte den Beschwerdeführer, dass sie einen Subdienstleister zur Konfliktlösung betrauen werde und sich dieser mit dem Beschwerdeführer in Verbindung setzen werde. Der Beschwerdeführer teilte der Mitarbeiterin daraufhin mit, dass seine Kon¬taktdaten nicht an den Subdienstleister übermittelt werden sollen und er auch keine Kontaktaufnahme durch Dritte wünsche. Da der Beschwerdeführer am nächsten Tag dennoch vom Subdienstleister telefonisch kontaktiert wurde, erachtete sich der Beschwerdeführer durch die Weitergabe seiner Namens- und Telefondaten von der Hausverwaltung in seinem Recht auf Geheimhaltung als verletzt und erhob Beschwerde bei der Datenschutzbehörde.

Im Rahmen des Verfahrens vor der Datenschutzbehörde brachte die Hausverwaltung vor, dass die Datenübermittlung an den Subdienstleister durch die einschlägigen landesgesetzlichen Bestimmungen gedeckt gewesen wäre. Das entsprechende Gesetz sieht in der Tat vor, dass die Hausverwaltung sowie der Subdienstleister für die Erhebung eines Sachverhaltes bezüglich der Gewährleistung des friedlichen Zusammenlebens und der raschen Konfliktlösung berechtigt sind, einander Auskünfte zu erteilen bzw. in diesem Zusammenhang personenbezogene Daten der Mieterinnen und Mieter auszutauschen. Da die Übermittlung der Daten des Beschwerdeführers von der Hausverwaltung an den Subdienstleister somit gesetzlich gedeckt war, wies die Datenschutzbehörde die Beschwerde ab.

Dieser Bescheid ist rechtskräftig.

6. Bescheid vom 25.02.2020, GZ: 2020-0.103.803(Geheimhaltung, Rechtmäßigkeit der Verarbeitung, Information, Informationspflicht, militärischer Eigenschutz, Verlässlichkeitsprüfung, Verlässlichkeitserklärung, Daten Angehöriger, Dateisystem, Übergangsfall)

Der Bruder der Beschwerdeführerin ist Angehöriger des österreichischen Bundesheeres. Beschwerdegegner ist das Bundesministerium für Landesverteidigung/ Abwehramt.

Der Bruder der Beschwerdeführerin gab anlässlich der Begründung eines Dienstverhältnisses im Rahmen einer „Verlässlichkeitsprüfung" eine „erweiterte Verlässlichkeitserklärung" ab. Dabei wurden auch Name, Geburtsort und -datum, Staatsbürgerschaft, Beruf und Wohnsitz der Schwester aufgenommen. Der Beschwerdegegner verarbeitete die Daten der Beschwerdeführerin nicht elektronisch, sondern sind diese Teil eines Papieraktes.

Da die Beschwerde vor dem 25.05.2018 bei der Datenschutzbeschwerde eingebracht wurde, war materiellrechtlich - in Bezug auf Geheimhaltung - auf den Zeitpunkt der Rechtsverletzung abzustellen und daher die alte Rechtslage, das DSG 2000, anzuwenden. Die Datenschutzbehörde führte aus, dass der Beschwerdegegner, der eine Behörde ist, nicht mehr Daten der Beschwerdeführerin erhoben hat, als im Militärbefugnisgesetz samt dazugehöriger Verordnung über die Verlässlichkeitserklärung vorgesehen. Deshalb lag keine Verletzung im Recht auf Geheimhaltung vor.

Hinsichtlich der Informationspflichten des Beschwerdegegners führte die Datenschutzbehörde zunächst aus, dass materiellrechtlich die neue Rechtslage - das DSG - anzuwenden sei, weil der Beschwerdegegner die Beschwerdeführerin auch über den 25.05.2018 hinaus nicht über die Erhebung der Daten informiert hatte.

Die Erhebung der Daten fällt unter das 3. Hauptstück des DSG, weil sie durch eine zuständige Behörde für Zwecke der militärischen Eigensicherung erfolgte. Das 3. Hauptstück des DSG setzt die Richtlinie (EU) 2016/680 um. Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Die Datenschutzbehörde entschied hier, dass es sich beim Beiblatt, das die Daten der Beschwerdeführerin beinhaltet, und Teil eines – ihren Bruder betreffenden – Gesamtkonvolutes ist, nicht um ein „Dateisystem" handelt, da die Daten der Beschwerdeführerin darin nicht leicht auffindbar sind. Eine Verletzung der Informationspflichten seitens des Beschwerdegegners lag daher nicht vor.

Dieser Bescheid ist rechtskräftig.

7. Bescheid vvom 28.02.2020, GZ: DSB-D123.685/0009-DSB/2019 (Veröffentlichung von Bildaufnahmen der Polizei während einer Amtshandlung)

Hier hatte sich die Datenschutzbehörde mit der Frage zu befassen, inwiefern das Filmen von Organen des öffentlichen Sicherheitsdienstes während einer Amtshandlung und das anschließende Veröffentlichen dieser Bildaufnahmen auf sozialen Medien gegen das Recht der Polizisten auf Geheimhaltung verstößt. Hierbei hatte die Datenschutzbehörde den Schutz auf personenbezogene Daten gegen das Recht auf freie Meinungsäußerung abzuwägen und gelangte zu einer teilweisen Stattgabe der Beschwerde.

Das Hinterfragen der Verhältnismäßigkeit von polizeilicher Befehls- und Zwangsgewalt – hier zum Thema „Ethnic Profiling durch die Polizei" – stellt einen Beitrag zu einer Debatte von öffentlichem Interesse dar.

Es lag daher nach Ansicht der Datenschutzbehörde grundsätzlich eine zulässige Veröffentlichung vor und war die Beschwerde dahingehend abzuweisen.

Anders verhält es sich jedoch bei zwei konkreten Bildaufnahmen: Zum einen wurde ein Polizist, unter Verwendung eines Snapchat-Filters, mit Hasenohren und Hasennase dargestellt, zum anderen wurde eine Polizistin abgelichtet, wobei diese Bildaufnahme mit anzüglichem Text und sexualisiertem Emoji versehen war. Diese beiden Veröffentlichungen stellen keinen geeigneten Beitrag zu einer Debatte von öffentlichem Interesse dar. Insbesondere liegt in letzterer Bildaufnahme der Fokus nicht auf einem Organ der Polizei, sondern bezieht sich direkt auf eine Person in ihrer Rolle als Frau. Im Hinblick auf diese beiden Bildaufnahmen überwiegt daher das Recht auf Geheimhaltung und war der Beschwerde dahingehend stattzugeben.

Dieser Bescheid ist rechtskräftig.

8. Bescheid vom 18.03.2020, GZ: 2020-0.008.056 (Bildverarbeitung „neu“ im privaten Bereich)

Die Beschwerdeführerin und die Beschwerdegegnerin sind Nachbarinnen und bewohnen gegenüberliegende Grundstücke. Der Garteneingang der Beschwerdeführerin liegt dabei jenem der Beschwerdegegnerin direkt gegenüber. Am Garteneingang der Beschwerdegegnerin ist eine Gegensprechvorrichtung mit integrierter Kamera angebracht. Die Beschwerdeführerin erachtete sich durch die Videoüberwachung der Beschwerdegegnerin in ihrem Recht auf Geheimhaltung als verletzt.

Die Datenschutzbehörde wies die Beschwerde ab. Sie begründete dies damit, dass die Videoüberwachung gemäß Art 6 Abs. 1 lit f DSGVO rechtmäßig ist: Im konkreten Fall war das berechtigte Interesse der Beschwerdegegnerin der Schutzzweck, dh.: das Erkennen-Können von potentiellen Gefahren vor Öffnen des Gartentores bzw. vor Verlassen des Hauses. Die Datenverarbeitung (hier: die Videoüberwachung) war zur Verwirklichung ihres Interesses auch erforderlich, da die Beschwerdegegnerin aufgrund ihres Sichtschutzes am Gartenzaun, aus ihrem Fenster etwaige Besucher nicht sehen konnte. Die Datenschutzbehörde führte dazu aus, dass eine Umgestaltung des Zaunes außer Verhältnis stünde bzw unzumutbar wäre. Den Geheimhaltungsinteressen der Beschwerdeführerin überwogen hier die Interessen der Beschwerdegegnerin, potenzielle Gefahren vor Öffnen der Türe erkennen zu können. Außerdem handelte es sich um eine bloße Echtzeitüberwachung und erfolgen die Aufnahmen nicht durchgehend.

Dieser Bescheid ist nicht rechtskräftig.

9. Bescheid vvom 20.03.2020, GZ: DSB-D124.881/0003-DSB/2019 (Auskunftsrecht versus anwaltliche Verschwiegenheitspflicht)

Der Beschwerdeführer verlangte Auskunft vom Beschwerdegegner, einem Anwalt, der eine Gemeinde vertrat, die mit dem Beschwerdeführer mehrere Rechtsstreite führt. Im vorliegenden Fall hatte der Beschwerdeführer aber weitere Rechtsstreite gegen die vom Beschwerdegegner vertretene Gemeinde angekündigt. Der Beschwerdegegner erteilte dem Beschwerdeführer unter Hinweis auf die aktuellen und noch zu führenden Rechtsstreitigkeiten zwischen seiner Mandantin - der Gemeinde - und dem Beschwerdeführer sowie aufgrund seiner anwaltlichen Verschwiegenheitspflicht keine Auskunft.

Nach der Judikatur des BVwG ist ein pauschaler Hinweis auf die anwaltliche Verschwiegenheitspflicht gemäß § 9 Abs. 2 RAO als Begründung für die Nichterteilung einer Auskunft unzulässig.

Die Datenschutzbehörde entschied, dass hier eine vollständige Auskunftserteilung die Prozesssituation der Mandantin und auch die Ausübung der Anwaltschaft durch den Beschwerdegegner negativ beeinträchtigen könnte. Der Beschwerdegegner musste dem Beschwerdeführer daher nur Stammdaten (wie Name, Titel und Adresse), nicht aber sonstige Informationen beauskunften.

Dieser Bescheid ist nicht rechtskräftig.

10. Bescheid vom 25.03.2020, GZ: DSB-D123.947/0003-DSB/2019 (Inhalt eines Bescheides als personenbezogenes Datum gemäß Art 4 Z 1 DSGVO)

Die Beschwerdegegnerin - eine Gemeinde - hatte einen Bescheid, den sie nicht selbst erlassen hatte, sondern nur zu Information erhalten hatte, ebenfalls zur Information an einen Dritten weitergegeben. Der Bescheid war gegen den Beschwerdeführer als Betreiber einer Wasserversorgungsanlage gerichtet und sprach aus, dass das Wasser nicht als Trinkwasser geeignet ist. Der Bescheid trug dem Beschwerdeführer als Sofortmaßnahme auf, betroffene Verbraucher über die mangelhafte Trinkwasserqualität in Kenntnis zu setzen. Die Gemeinde übermittelte diesen Bescheid zur Information an einen Verbraucher, der sich dazu bei ihr erkundigt hatte.

Die Datenschutzbehörde führte dazu aus, dass nicht nur die im Bescheid enthaltenen konkreten Informationen wie Name, Adresse und Wohnort des Beschwerdeführers personenbezogene Daten sind. Vielmehr ist der Inhalt des Bescheides an sich als personenbezogenes Datum gemäß Art. 4 Z 1 DSGVO zu qualifizieren, zumal der Bescheid, als individueller Rechtsakt, gegenüber dem Beschwerdeführer persönlich ergangen ist und daher Informationen über den Beschwerdeführer aufweist.

Die Datenschutzbehörde gab der Beschwerde statt, weil die Übermittlung an den Dritten durch die Beschwerdegegnerin nicht gesetzlich vorgesehen ist. Auch hätte der Verbraucher durch die Beschwerdegegnerin durch ein gelinderes Mittel informiert werden können.

Dieser Bescheid ist nicht rechtskräftig.

11. Bescheid vom 21.04.2020, GZ: DSB-D124.1210/0004-DSB/2019 (Nach erteilter Auskunft ist Löschung wegen Widerruf zulässig; Beauskunftung von Empfängerkategorien oder konkreten Empfängern, Einzelheiten zu Profiling müssen erteilt werden)

Der Beschwerdeführer verlangte Auskunft vom Beschwerdegegner, einer Gesellschaft für Lebensmittel-Großhandel. Der Beschwerdeführe war Mitglied in einem „Club" der Beschwerdegegnerin, der Vorteile wie vergünstigte Lebensmittelpreise bot. In seinem Auskunftsantrag kündigte der Beschwerdeführer nun seine Mitgliedschaft mit sofortiger Wirkung und widerrief die Zustimmung zur Verwendung seiner Daten.

Die Beschwerdegegnerin erteilte in Folge Auskunft, die der Beschwerdeführer aber wegen Nennung der bloßen Empfängerkategorien (hier: Druckereien, Transport/Logistik,…) - statt konkreter Empfänger - für unvollständig hielt. Auch beanstandete der Beschwerdeführer fehlende Informationen zum vom Beschwerdegegner betriebenen Profiling. Nach erteilter Auskunft löschte der Beschwerdegegner die Daten des Beschwerdeführers, was der Beschwerdeführer kritisierte.

Die Datenschutzbehörde entschied hier, dass der Beschwerdegegner die konkreten Empfänger beauskunften muss. Bei einer Interessenabwägung zwischen dem nicht weiter begründungsbedürftigen Auskunftsinteresse des Beschwerdeführers gegen das Geheimhaltungsinteresse an der Nicht-Nennung der konkreten Empfänger überwog das Auskunftsinteresse des Beschwerdeführers wegen fehlender schutzwürdiger Interessen des Beschwerdegegners.

Zum Profiling entschied die Datenschutzbehörde, dass der Beschwerdegegner auch die zur Profilerstellung verwendeten Eingabedaten und die Informationen zum Profil und Details zu den Segmenten, in die der Beschwerdeführer eingeteilt wurde, mitteilen muss.

Da der Beschwerdegegner die Daten des Beschwerdeführers gelöscht hat, weil letzterer seine Zustimmung widerrufen hat, verhielt sich der Beschwerdegegner DSGVO-konform. Die Löschung war rechtmäßig.

Dieser Bescheid ist rechtskräftig.

12. Bescheid vom 21.04.2020, GZ: 2020-0.239.741 (Medienprivileg, Löschung, Medien, Medienunternehmen, Medienberichterstattung, Medieninhalt, Informationsfreiheit, Unzuständigkeit der Datenschutzbehörde)

Der Beschwerdeführer beschwerte sich im Recht auf Löschung gegen die Betreiberin einer Online-Tageszeitung. Diese berichtete in einem Online-Artikel über das dokumentierte Verhalten des Beschwerdeführers am Telefon gegenüber einem Mitarbeiter des Polizeinotrufs, das zum Gegenstand von Spott in verschiedenen Sozialen Medien gemacht wurde. Weiters ist in diesem Online-Artikel ein YouTube-Video eingebettet, das den Anruf des Beschwerdeführers, der eine Leitungsfunktion bei der österreichischen Polizei innehatte, beim Polizeinotruf wiedergibt. Unterhalb des Online-Artikels sind Twitter-Beiträge eingebettet, die Bezug auf diesen Polizeinotruf-Gesprächsmitschnitt nehmen.

Die Datenschutzbehörde entschied, dass hier das sogenannte „Medienprivileg" zur Anwendung gelangt: Da es sich bei der Berichterstattung der Online-Tageszeitung um eine Datenverarbeitung „zu journalistischen Zwecken des Medienunternehmens" handelt, ist § 9 Abs. 1 DSG erfüllt. Die Datenschutzbehörde ist daher unzuständig, inhaltlich über die Beschwerde zu entscheiden. Vielmehr sind nur die ordentlichen Gerichte für eine inhaltliche Entscheidung zuständig.

Primär sollte der Online-Artikel die Öffentlichkeit über Missstände in der Verwaltung aufklären. Eine darin auch vorgenommene Verächtlichmachung - der Beschwerdeführer sei eine „Lachnummer"- ist deshalb von der Freiheit auf Meinungsäußerung geschützt, weil sie als stilistisches Mittel bloß als „Nebenzweck" darauf abzielt, zu provozieren oder zu schockieren.

Dieser Bescheid ist rechtskräftig.

13. Bescheid vom 24.04.2020, GZ: 2020-0.219.620 (Auskunft, Umfang des Auskunftsrechts, Einzelhandelsunternehmen, Optiker, Nachholung der Auskunftserteilung, Marketing und Werbung, kein Recht auf Auskunft über Zeitpunkte des Datenaustausches mit Auftragsverarbeiter)

Der Beschwerdegegner erteilte auf mehrmalige Nachfrage des Beschwerdeführers mehrmalig ergänzende Auskunft. Der Beschwerdeführer beschwerte sich dennoch wegen Unvollständigkeit der ihm erteilten Auskunft.

Die Rechtsfrage, die sich hier stellte, war, ob der Beschwerdegegner und datenschutzrechtliche Verantwortliche auch die Auftragsverarbeiter, sowie die durch ihn an den Auftragsverarbeiter offengelegten Daten und den Zeitpunkt der Offenlegung beauskunften muss.

Die Datenschutzbehörde entschied, dass der Auftragsverarbeiter als Empfänger gilt, der gemäß Art. 15 Abs. 1 lit. c DSGVO zu beauskunften ist. Dies gilt auch für die vom Verantwortlichen an den Auftragsverarbeiter offengelegten Daten. Ein Recht, auch den Zeitpunkt der Offenlegung

der an den Auftragsverarbeiter offengelegten Daten beauskunftet zu bekommen, ist jedoch nicht aus Art. 15 DSGVO ableitbar.

Die Datenschutzbehörde wies die Beschwerde ab.

Dieser Bescheid ist rechtskräftig.

14. Bescheid vom 20.05.2020, GZ: 2020-0.251.582 (Unerlaubte Einsichtnahme in Patientenakt)

Die Datenschutzbehörde setzte sich hier mit dem Vorwurf der unerlaubten Einsichtnahme eines Ordinationsgehilfen in den Patientenakt eines Betroffenen auseinander. Die Beschwerdeführerin brachte in ihrer Beschwerde zunächst vor, dass sie sich bei der Beschwerdegegnerin in ärztlicher Behandlung befunden habe. Aufgrund eines versäumten Arzttermins sei es zwischen ihr und dem Ordinationsgehilfen der Beschwerdegegnerin zu einem Disput gekommen und habe sie in der Folge eine negative Bewertung zur Beschwerdegegnerin im Internet abgegeben. Daraufhin, so der Verdacht der Beschwerdeführerin, habe der Ordinationsgehilfe Einsicht in ihre Patientenakte genommen, um so die Daten ihres Arbeitgebers ausfindig zu machen, um selbst im Internet eine negative Bewertung zur Beschwerdeführerin abzugeben. Im Rahmen des Verfahrens vor der Datenschutzbehörde brachte die Beschwerdegegnerin bzw. der Ordinationsgehilfe vor, dass die abgegebene Bewertung nicht im Zusammenhang mit der Beschwerdeführerin stehen würde, sondern eine andere Mitarbeiterin des Arbeitgebers der Beschwerdeführerin gemeint gewesen wäre.

Nach der Durchführung des Ermittlungsverfahrens sah es die Datenschutzbehörde als erwiesen an, dass die Bewertung des Ordinationsgehilfen gegen die Beschwerdeführerin gerichtet war. Darüber hinaus sah es die Datenschutzbehörde als erwiesen an, dass der Ordinationsgehilfe Einsicht in den Patientenakt der Beschwerdeführerin genommen hatte, da es sich bei der Information hinsichtlich des Arbeitgebers der Beschwerdeführerin um keine im Internet abrufbare Information handelte und auch die Datenschutzbehörde im Rahmen einer amtswegigen Recherche den Arbeitgeber der Beschwerdeführerin nicht eruieren konnte. Der Beschwerde wurde daher stattgegeben und festgestellt, dass die Beschwerdeführerin in ihrem Recht auf Geheimhaltung verletzt wurde.

Dieser Bescheid ist rechtskräftig.

15. Bescheid vom 25.05.2020, GZ: 2020-0.191.240 (Geheimhaltung, Rechtmäßigkeit der Verarbeitung, juristische Person, Verantwortlicher, Beschwerdelegitimation, Aufsichtsbehörde, Arzneimittel-Großhandel, Betriebsprüfung, Ermittlungsverfahren, Beweismittel, Relevanz, Übermaßverbot, amtswegige Löschungspflicht)

Die Beschwerdeführerin ist eine Gesellschaft, die als Arzneimittelgroßhändler tätig ist, und wurde vom Beschwerdegegner, dem Bundesamt für Sicherheit im Gesundheitswesen, einer Betriebsprüfung nach § 68 AMG unterzogen. Dabei sah der Beschwerdegegner Unterlagen der Beschwerdeführerin ein, vervielfältigte sie und wurden Daten der Beschwerdeführerin an Dritte weitergegeben. Die Beschwerdeführerin machte eine Verletzung im Recht auf Geheimhaltung gemäß § 1 DSG bei der Datenschutzbehörde geltend.

Zunächst stellte sich der Datenschutzbehörde hier die Frage der Antragslegitimation der Beschwerdeführerin, da es sich bei dieser um keine natürliche, sondern um eine juristische Person handelt. Die Datenschutzbehörde führte aus, dass § 1 DSG auch juristische Personen schützt und diese eine Beschwerde nach § 24 DSG vor der Datenschutzbehörde erheben können, sofern sie eine Verletzung der durch § 1 DSG gewährleisteten Rechte behaupten.

Inhaltlich entschied die Datenschutzbehörde, dass das sogenannte „Übermaßverbot“ hier zur Anwendung gelangt: Wenn es denkmöglich ist, dass die von einer in der Sache zuständigen Behörde ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet sind, ist die Zulässigkeit der Ermittlung aus datenschutzrechtlicher Sicht gegeben. Demnach war durch die vom Beschwerdegegner im Zuge der Betriebsprüfung verarbeiteten Daten der Beschwerdeführerin keine Verletzung von § 1 DSG gegeben.

Die Datenschutzbehörde entschied weiters, dass auch in Bezug auf die Unterlassung einer Löschung bzw. einer Vernichtung von personenbezogenen Daten der Beschwerdeführerin keine Verletzung im Recht auf Geheimhaltung nach § 1 Abs. 1 DSG vorlag, da der Beschwerdegegner die Daten nicht länger als notwendig aufbewahrt hatte.

Dieser Bescheid ist rechtskräftig.

16. Bescheid vom 28.05.2020, 2020-0.280.699 (Verletzung im Recht auf Geheimhaltung: Verarbeitung eines Lichtbildausweises aufgrund eines Geldwechsels im Gegenwert von 100 Euro)

Die Datenschutzbehörde setzte sich hier mit einer Beschwerde im Recht auf Geheimhaltung und dem Finanzmarkt-Geldwäschegesetz (FM-GwG) auseinander. Der Beschwerdeführer wollte in einer Bankfiliale 100 Euro in Türkische Lira (TRY) wechseln lassen. Daraufhin wurde er vom Bankmitarbeiter aufgefordert, einen Lichtbildausweis für den Wechsel vorzulegen, bei sonstigem Abbruch des Geldwechsels. Der Beschwerdeführer weigerte sich vorerst, aber schließlich legte er seinen Führerschein vor, welcher kopiert und gespeichert wurde. Die Bank als Beschwerdegegnerin begründete die gegenständliche Verarbeitung des Lichtbildausweises mit ihren Obliegenheiten aufgrund des FM-GwG. Demnach habe sie ohne Rücksicht auf die Höhe des ein- und auszahlenden Betrages, bei bloßem Verdacht hinsichtlich Geldwäsche oder Terrorismusfinanzierung (§ 5 Z 4 FM-GwG) Sorgfaltsmaßnahmen anzuwenden und im Zweifel Identitätsdokumente gemäß § 6 Abs. 1 Z 1 FM-GwG zu verlangen. Seine Weigerung sei als auffälliges Kundenverhalten interpretiert worden. Darüber hinaus sei es dem Bankfilialleiter erinnerlich gewesen, dass der Beschwerdeführer bei einer höheren Bundesbehörde gearbeitet habe, daher sei gemäß § 2 Z 6 iVm § 11 FM-GwG eine PeP (Politisch exponierte Person) Prüfung durchzuführen gewesen.

Die Datenschutzbehörde gab der Beschwerde statt und stellte eine Verletzung im Recht auf Geheimhaltung fest, da es sich bei dem Geldwechsel des Beschwerdeführers im Gegenwert von 100 Euro jedenfalls um einen Betrag unterhalb der Wertgrenze von 1.000 Euro, bzw. 15.000 Euro des § 5 Z 2 FM-GwG handle. Weiters kann allein aus einer Weigerung, einen Lichtbildausweis vorzulegen, noch nicht geschlossen werden, dass es sich bei einem Geldwechsel um Terrorismusfinanzierung oder Geldwäsche handelt. Darüber hinaus ist ein Bediensteter einer höheren Bundesbehörde nicht gleichbedeutend mit einer politisch exponierten Person, wonach es sich beispielsweise um Staatschefs, Parlamentsabgeordnete oder Verfassungsrichter handle. Daher lag keine Rechtfertigung für die gegenständliche Verarbeitung von personenbezogenen Daten vor.

Dieser Bescheid ist nicht rechtskräftig.

17. Bescheid vom 12.06.2020, GZ: 2020-0.225.643 (Geheimhaltung, Versicherungsunternehmen, Versicherungsfall, Leistungspflicht, Datenermittlung, Gesundheitsdaten, Medikamentenbezug, Apothekenbelege, Belegeobliegenheit, Übergangsfall)

Der Beschwerdeführer behauptete eine Verletzung im Recht auf Geheimhaltung, weil die Beschwerdegegnerin – eine Versicherung, bei der der Beschwerdegegner eine Zusatzversicherung abgeschlossen hatte – von ihm Apothekenbelege im Original verlange. Die Apothe-

kenbelege würden aber den Namen des Medikaments enthalten und somit Rückschlüsse auf seine Krankheit zulassen, was die Beschwerdegegnerin nichts angehe.

Da die Apothekenbelege Aufschluss über die Gesundheit des Beschwerdeführers geben, sind sie sensible Daten. Diese durften - nach alter Rechtslage des DSG 2000 - nur verwendet werden, wenn ein Gesetz, das der Wahrung wichtiger öffentlicher Interessen dient, dies vorsieht. Nun war in § 34 VersVG vorgesehen, dass der Versicherungsnehmer zur Erteilung von Auskünften an den Versicherer verpflichtet ist, wenn dies zur Feststellung des Versicherungsfalles oder des Umfanges der Leistungspflicht des Versicherers erforderlich ist.

Die Datenschutzbehörde hatte nun zu prüfen, ob es notwendig war, dass der Beschwerdeführer die Apothekenbelege – unter Nennung des Medikamentennamens – der Beschwerdegegnerin vorlegte. Die Beschwerdegegnerin führte dazu aus, dass durch eine bloße Rezeptgebührenbestätigung - wie sie der Beschwerdeführer für ausreichend hielt - eventuelle irrtümliche Doppeleinreichungen nicht festgestellt und dadurch eine korrekte Bearbeitung durch die Mitarbeiter der Versicherung im Interesse der Gesamtversichertengemeinschaft nicht garantiert werden könne. Aufgrund dessen entschied die Datenschutzbehörde, dass es „denkmöglich" ist, dass die Versicherung die Apothekenbelege benötige und verneinte eine Rechtsverletzung.

Dieser Bescheid ist rechtskräftig.

18. Bescheid vom 29.06.2020, GZ: 2020-0.396.410 (Auskunftsrecht eines gerichtlich bestellten psychologischen Sachverständigen)

Hier beschäftigte sich die Datenschutzbehörde mit einem Auskunftsbegehren, gerichtet an einen gerichtlich bestellten psychologischen Sachverständigen. Der Beschwerdegegner wurde vom zuständigen Landesgericht für Strafsachen im Verfahren gegen den Beschwerdeführer als psychologischer Sachverständiger bestellt und mit der Erstellung eines Gutachtens zum Beschwerdeführer beauftragt. Nach der Übermittlung des Gutachtens an das Landesgericht, wandte sich der Beschwerdeführer mit einem Auskunftsbegehren an den Beschwerdegegner. Der Beschwerdegegner kam dem Auskunftsbegehren nicht nach, sondern verwies darauf, dass er als gerichtlich bestellter Sachverständiger funktioneller Teil der Rechtspflege sei, weshalb auch die Strafprozessordnung auf ihn anzuwenden wäre. Die Strafprozessordnung würde Parteien die Gelegenheit zur Akteneinsicht geben, eine Akteneinsicht beim Gutachter sei hingegen nicht vorgesehen.

Die Datenschutzbehörde verwies in ihrer Entscheidung zunächst auf die Judikatur des Bundesverwaltungsgerichts, wonach gerichtlich beeidete Sachverständige zumindest gemeinsam mit dem Gericht, das sie mit der Gutachtenserstellung beauftragt hat, als Verantwortliche im Sinne des Art. 4 Z 7 DSGVO zu betrachten sind. Die Datenschutzbehörde verwies sodann darauf, dass die Bestellung des Beschwerdegegners zwar im Rahmen eines anhängigen Strafverfahrens geschehen sei, allerdings bei der Gutachtenerstellung von keiner „justiziellen Tätigkeit" ausgegangen werden kann, weshalb die Datenschutzbehörde auch zur Entscheidung zuständig ist.

Während in der DSGVO Daten in Patientenakten, Informationen wie Diagnosen, Untersuchungsergebnisse oder Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen ausdrücklich vom Recht auf Auskunft als umfasst angesehen werden, hat der österreichische Gesetzgeber im Psychologengesetz 2013 keine Beschränkung für das Recht auf Auskunft vorgesehen. Da die DSGVO auch keine Einschränkung des Rechts auf Auskunft zugunsten eines gesetzlich normierten (Akten)Einsichtsrechts vorsieht, kam die Datenschutzbehörde zum Ergebnis, dass der Beschwerdegegner gegenüber dem Beschwerdeführer zur Auskunfts-

erteilung verpflichtet ist und der Beschwerdegegner dem Beschwerdeführer eine dem Art. 15 DSGVO entsprechende Auskunft zu erteilen hat.

Die Beschwerde ist rechtskräftig.

19. Bescheid vom 09.07.2020, GZ: 2020-0.127.361 (Einladung zur Akteneinsicht als Reaktion auf ein Auskunftsbegehren)

Hier befasste sich die Datenschutzbehörde mit der Frage, ob die Beschwerdegegnerin den Beschwerdeführer dadurch im Recht auf Auskunft verletzt hat, indem sie ihn in Reaktion auf ein Auskunftsbegehren zur Akteneinsicht eingeladen hat. Der Beschwerdeführer richtete ein Auskunftsbegehren an die Beschwerdegegnerin und beantragte darin „volle Auskunft über seine personenbezogenen Daten". Die Beschwerdegegnerin beantwortete das Auskunftsbegehren, indem sie den Beschwerdeführer zur Akteneinsicht einlud und ihm diesbezüglich einen Termin mitteilte. Weiters wurde der Beschwerdeführer darüber informiert, dass er sich gemäß § 17 AVG von Akten oder Aktenteilen an Ort und Stelle Abschriften selbst anfertigen und auf seine Kosten Kopien oder Ausdrucke erstellen lassen könne. Der Beschwerdeführer ist zu dem im Schreiben genannten Termin nicht erschienen. Die Beschwerdegegnerin benachrichtigte daraufhin den Beschwerdeführer mit Schreiben, dass aufgrund des unentschuldigten Nichterscheinens das „Datenauskunftsverfahren" eingestellt werde.

Die Datenschutzbehörde gab der Beschwerde statt und trug der Beschwerdegegnerin auf, dem Beschwerdeführer eine dem Art. 15 DSGVO entsprechende Auskunft zu erteilen. Die Datenschutzbörde begründete dies zunächst damit, dass der DSGVO eine Subsidiaritätsregelung, wie sie in § 44 Abs. 5 DSG im Anwendungsbereich des 3. Hauptstücks des DSG (welches gegenständlich nicht zur Anwendung kommt) vorgesehen ist, fremd ist. Daraus ist abzuleiten, dass nunmehr mittels eines Auskunftsbegehrens grundsätzlich auch Auskunft über den Inhalt von Urkunden und Aktenbestandteilen begehrt werden kann, sofern darin personenbezogene Daten der betroffenen Person enthalten sind und der sachliche Anwendungsbereich der DSGVO eröffnet ist. Ein Verantwortlicher hat gemäß Art. 12 Abs. 1 DSGVO geeignete Maßnahmen zu treffen, um einer betroffenen Person alle Informationen gemäß den Art. 13 und 14 DSGVO und alle Mitteilungen gemäß den Art. 15 bis 22 und Art. 34 DSGVO, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Diese Informationen sind gemäß Art. 12 Abs. 3 DSGVO unverzüglich, in jedem Fall aber innerhalb eines Monats nach Antrag zur Verfügung zu stellen. Die Beschwerdegegnerin reagierte daher jedenfalls unzureichend auf das Auskunftsbegehren, weshalb seitens der Datenschutzbehörde eine Rechtsverletzung festgestellt wurde und der Beschwerdegegnerin ein entsprechender Leistungsauftrag erteilt wurde.

Dieser Bescheid ist rechtskräftig.

20. Bescheid vom 10.08.2020, GZ: 2020-0.204.456 (Geheimhaltung, Auskunft, Rechtmäßigkeit der Verarbeitung, Unterhaltsstreit, Scheidungsverfahren, Haushaltsausnahme, E-Mails, Kontaktdaten, SMS, WhatsApp-Nachrichten, heimliche Tonaufnahmen, Recht auf Datenkopie, Beweismittel, Beweisnotstand)

Die Beschwerdeführerin und der Beschwerdegegner befanden sich in einem streitigen Scheidungs- und Unterhaltsverfahren.

Die Beschwerdeführerin machte ihr Recht auf Geheimhaltung und Auskunft bei der Datenschutzbehörde geltend. Der Beschwerdegegner entgegnete, dass die DSGVO nicht auf den Fall der Beschwerdeführerin anzuwenden sei, weil die SMS-, WhatsApp-Nachrichten und Tonband-

aufnahmen, die er von der Beschwerdeführerin hatte, „ausschließlich persönlichen oder familiären Tätigkeiten“ gemäß Art. 2 Abs. 2 lit c DSGVO dienen würden.

Die Datenschutzbehörde entschied, dass die DSGVO sehr wohl anzuwenden ist, weil der Beschwerdegegner den SMS/WhatsApp-Verkehr sowie die Tonbandaufnahmen nicht für „persönliche oder familiäre Tätigkeiten“ verarbeite, sondern um sie im Scheidungsverfahren gegen die Beschwerdeführerin zu verwenden.

Die Datenschutzbehörde entschied weiters, dass die heimliche Anfertigung von Tonbandaufnahmen der Beschwerdeführerin hier unrechtmäßig ist. Beim Beschwerdegegner lag nämlich kein Beweisnotstand in dem Sinn vor, dass er die Tonaufzeichnungen bei sonstiger Undurchsetzbarkeit seines Anspruchs unbedingt benötigte: Der Beschwerdegegner führte vielmehr aus, dass er – wenn die Beschwerdeführerin der Vorlage vor Gericht nicht zustimmen würde – eine monatelange gerichtliche Einvernahme dieser Beschwerdeführerin abwarten würde.

Der österreichische Gesetzgeber hat keine Bestimmungen erlassen, die es dem Empfänger eines Auskunftsantrages zwecks „Durchsetzung zivilrechtlicher Ansprüche“ erlauben, die zu erteilende Auskunft nicht oder nur eingeschränkt zu erteilen. Deshalb muss der Beschwerdegegner der Beschwerdeführerin gemäß Art. 15 Abs. 1 und 2 DSGVO Auskunft erteilen.

Die Beschwerdeführerin hat aber keinen Anspruch auf Herausgabe einer Kopie von Dokumenten, sondern nur auf „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind“. Ganze Tonbandaufnahmen und SMS/WhatsApp-Verläufe musste der Beschwerdegegner der Beschwerdeführerin also nicht herausgeben.

Dieser Bescheid ist rechtskräftig.

21. Bescheid vom 21.08.2020, GZ: 2020-0.208.921 (Veröffentlichung personenbezogener Daten im Rahmen von Wahlwerbung)

Im gegenständlichen Fall hatte sich die Datenschutzbehörde mit der Frage zu beschäftigen, ob eine Verletzung im Recht auf Geheimhaltung im Rahmen der Versendung von Wahlwerbung vorliegt. Der Beschwerdeführer erhob Beschwerde bei der Datenschutzbehörde, da die Beschwerdegegnerin, eine wahlwerbende Partei, im Rahmen einer Vorwahl die Versendung eines Flugblattes an etwa 1500 Wahlberechtigte veranlasste und hierbei das gesamte Wählerverzeichnis einer Marktgemeinde beilegte, wodurch Name, Adresse und Geburtsjahr des Beschwerdeführers allen Wahlberechtigten offengelegt wurden. Die Beschwerdegegnerin berief sich auf Art. 6 Abs. 1 lit. f DSGVO und brachte vor, ein Verzeichnis aller wahlberechtigten Personen des Ortes sei für selbige von Interesse und diene der Offenlegung des Geburtsjahres und der Adresse der Unterscheidung namensgleicher Wähler.

Die Datenschutzbehörde hielt in ihrer Entscheidung fest, dass § 8 Abs. 1 Wählerkarteigesetz zwar für jedermann ein Einsichtsrecht zur Überprüfung der Vollständigkeit und Richtigkeit der Wählerkartei normiert, dies jedoch keine ausreichende Rechtsgrundlage für eine Offenlegung der dort enthaltenen Daten darstelle. Die dort normierte Zugänglichkeit auf die Daten des Beschwerdeführers senke zwar deren Schutzwürdigkeit, jedoch stelle das pauschale Vorbringen der Beschwerdegegnerin, die Offenlegung aller wählbaren Personen im Ort sei für Wahlberechtigte von großem Interesse und absoluter Wichtigkeit, kein ausreichend berechtigtes Interesse dar. Bei einem solchen Interesse der Wahlberechtigten haben diese gerade deshalb die in § 8 Abs. 1 Wählerkarteigesetz normierte Einsichtsmöglichkeit. Im Ergebnis war der Beschwerde daher stattzugeben, da eine Verletzung im Recht auf Geheimhaltung vorlag.

Dieser Bescheid ist nicht rechtskräftig.

22. Bescheid vom 01.09.2020, GZ: 2020-0.303.727 (Medienprivileg, Löschung, Verein, Berichterstattung zur Vereinstätigkeit, Redaktion, journalistischer Zweck, Medienunternehmen, Informationsfreiheit, Unzuständigkeit der Datenschutzbehörde)

In dieser Sache behauptete die Beschwerdeführerin durch die Berichterstattung auf der Website des Beschwerdegegners - eines Vereins, der sich u.a. für Tier- und Umweltschutz einsetzt - diffamiert und darin als „Spitzel" bezeichnet zu werden. Sie verlangte die Löschung der Berichterstattung. In der Berichterstattung ging es um einen Gerichtsprozess zwischen einem Jäger und dem Obmann des Vereins, in welchem die Beschwerdeführerin als Zeugin auftrat. Die Beschwerdeführerin war auch beim Verein tätig gewesen.

Die Datenschutzbehörde stellte u.a. fest, dass der Newsbereich der Website von 2 Chefredakteuren sowie weiteren 5 Redakteuren betreut wird, einmal pro Woche eine Redaktionssitzung stattfindet, alle Beiträge von der Chefredaktion genehmigt werden müssen und in den Betrieb des Newsbereichs rund 68 Wochenstunden investiert werden. Deshalb ging die Datenschutzbehörde davon aus, dass der Verein in diesem Fall als „Medienunternehmen" im Sinn der Judikatur des OGH angesehen werden kann.

Die Datenschutzbehörde ging auch davon aus, dass die Berichterstattung „zu journalistischen Zwecken" erfolgte, insbesondere weil es sich bei der Beschwerdeführerin um eine ehemalige Politikerin handelte und daher ein öffentliches Interesse an der Berichterstattung zu bejahen war.

Die Datenschutzbehörde wies die Beschwerde zurück, weil sie nicht für die inhaltliche Behandlung von Beschwerden zuständig ist, bei denen es um Datenverarbeitungen „zu journalistischen Zwecken durch ein Medienunternehmen" geht.

Dieser Bescheid ist rechtskräftig.

23. Bescheid vom 5.10.2020, GZ: 2020-0.535.661 (Verwendung einer Dashcam nicht überschießend)

Der Beschwerdeführer erachtete sich in seinem Recht auf Geheimhaltung als verletzt. Der Beschwerdeführer war mit einem KFZ auf einer Autobahn fahrend unterwegs gewesen. Dabei wurde er vom Beschwerdegegner, welcher zum gleichen Zeitpunkt einen Omnibus mit mehreren Personen an Bord hinter dem Beschwerdeführer lenkte, mittels Armaturenbrett-Kamera (auch: „Dashcam") gefilmt und wurde dabei eine 1 Minute und 56 Sekunden lange Aufnahme erstellt. Hintergrund der Aufzeichnung waren (versuchte) Überhol- und Bremsmanöver der Verfahrensparteien. Bei einem dieser Manöver bremste der Beschwerdeführer grundlos so stark ab, dass der hinter ihm fahrende Beschwerdegegner nur durch eine Notbremsung einen Auffahrunfall verhindert konnte. Auch in weiterer Folge versuchte der Beschwerdeführer durch unbegründetes Bremsen einen Auffahrunfall zu provozieren.

In Abkehr von ihrer bisherigen Rechtsansicht, wonach Dashcams per se unzulässig seien, vertritt die Datenschutzbehörde nunmehr die Ansicht, dass die Zulässigkeit einer Dashcam einzelfallbezogen zu erfolgen hat. Im vorliegenden Fall entschied die Datenschutzbehörde, dass dem Interesse des Beschwerdegegners an der Aufzeichnung der – relativ kurzen – Filmsequenz zum Nachweis eines Fehlverhaltens des Beschwerdeführers ein höheres Gewicht beizumessen ist, als dem Interesse des Beschwerdeführers, nicht gefilmt zu werden. Zu berücksichtigen war auch, dass die Filmsequenz als Beweismittel in einem vorangegangenen Strafverfahren gedient hatte, welche erst nach Zahlung einer Geldbuße durch den Beschwerdeführer mittels Diversion eingestellt worden war.

Dieser Bescheid ist nicht rechtskräftig.

24. Bescheid vom 23.10.2020, GZ: 2020-0.627.100 (Observierung durch Berufsdetektiv im höchstpersönlichen Lebensbereich überschießend)

Der Beschwerdeführer erachtete sich in seinem Recht auf Geheimhaltung als verletzt. Hintergrund des Falles war, dass er mit der Vermieterin seiner Wohnung in einen Mietrechtsstreit verwickelt war und diese zur Prüfung, ob Kündigungsgründe des Bestandsverhältnisses bestehen, eine Detektei engagiert hatte. Im Zuge dieses Mietrechtsstreits erfuhr der Beschwerdeführer, dass er von der Detektei observiert worden war und diese u.a. Fotos von ihm an und außerhalb von seinem Arbeitsplatz und in seiner Wohnung gemacht hatte. Die Detektei war Beschwerdegegnerin.

Weil die Identifizierung des Beschwerdeführers auf diesen Fotos durch Dritte nach allgemeinem Ermessen wahrscheinlich möglich ist, führte die Datenschutzbehörde aus, dass die Fotos personenbezogene Daten sind. Weiters qualifizierte die Datenschutzbehörde die Detektei als Verantwortlichen, da die Detektei zur Eruierung des [tatsächlichen] Wohnortes des Beschwerdeführers zwecks Dokumentation allfälliger mietrechtlicher Kündigungsgründe großen Ermessensspielraum bei der - mit der Datenverarbeitung verbundenen - Auswahl an Mittel hatte.

Die Datenschutzbehörde nahm in Folge eine Interessenabwägung vor: So standen die Geheimhaltungsinteressen des Beschwerdeführers an Fotoaufnahmen seiner Person dem Interesse der Beschwerdegegnerin an der Ausübung des Detektiv-Gewerbes sowie dem Interesse deren Auftraggeberin an der Dokumentation allfälliger (mietrechtlicher) Kündigungsgründe gegenüber. Die Datenschutzbehörde entschied, dass die Geheimhaltungsinteressen des Beschwerdeführers hinsichtlich jener Fotos, die ihn in seiner Wohnung und an seinem Arbeitsplatz zeigen, stärker wogen, weil er hier in seinem höchstpersönlichen Lebensbereich (an seinem Wohnsitz) bzw. an anderen geschützten Bereichen (seinem Arbeitsplatz) fotografiert worden war. Die Verwendung dieser Fotos war überschießend. Dies galt nicht für andere Fotos, die den Beschwerdeführer etwa auf dem Heimweg von seiner Arbeit zeigten: Hier wurde das Interesse der Beschwerdegegnerin als stärker qualifiziert; die Verwendung dieser Fotos war also rechtmäßig.

Dieser Bescheid ist nicht rechtskräftig.

25. Bescheid vom 03.11.2020, GZ: 2020-0.293.448 (Offenlegung der Adresse im Rahmen einer Beschwerdevorentscheidung durch das Finanzamt)

Gegenständlich beschwerte sich der Beschwerdeführer bei der Datenschutzbehörde wegen einer Verletzung im Recht auf Geheimhaltung gemäß § 1 DSG gegen ein Finanzamt, da dieses im Rahmen eines Abgabeverfahrens eine Beschwerdevorentscheidung an ein Bundesministerium, als auch an über 500 weitere Verfahrensparteien übermittelt hatte. Hierdurch wurden im Spruch der Beschwerdevorentscheidung der Name, die Adresse und der Wohnort des Beschwerdeführers ohne dessen Einwilligung offengelegt und seien diese Daten, laut dem Vorbringen des Beschwerdeführers, für die Zustellung der Beschwerdevorentscheidung nicht erforderlich gewesen. Der Beschwerdegegner brachte wiederum vor, § 48a Abs. 4 BAO erlaube eine Offenlegung dieser Daten, wenn dies der Durchführung eines Abgabeverfahrens diene, wie dies gegenständliche durch die Erlassung der Beschwerdevorentscheidung der Fall war.

Die Datenschutzbehörde qualifizierte den Beschwerdegegner als staatliche Behörde iS des § 1 Abs. 2 DSG und somit als datenschutzrechtlichen Verantwortlichen und hielt fest, dass der Beschwerdegegner grundsätzlich nach den Bestimmungen der BAO und des AVOG 2010 zur Erlassung einer Beschwerdevorentscheidung zuständig ist, womit das Bestehen einer gesetzlichen Aufgabe zu bejahen war. Das Anführen von Vor- und Zunamen des Beschwerdeführers im Spruch der Beschwerdevorentscheidung diene hierbei dessen eindeutiger Identifizierung und sei für die Erfüllung genannten gesetzlichen Aufgabe, daher für die Erlassung einer Beschwer-

devorentscheidung, erforderlich. Dies gelte jedoch nicht für die Offenlegung der Wohnadresse, weshalb es im gegenständlichen Fall zu einer teilweisen Stattgabe kam.

Dieser Bescheid ist rechtskräftig.

26. Bescheid vom 19.11.2020, GZ: 2020-0.743.659 (Wiener Contact Tracing Verordnung)
Im Zuge der Corona-Krise erließ der Magistrat der Stadt Wien (MA 15) am 28. September 2020 eine Verordnung betreffend Auskunftserteilung für Contact Tracing im Zusammenhang mit Verdachtsfällen von COVID-19. Zweck dieser Verordnung war es, die Verbreitung von COVID-19 durch Ausforschung allfällig infizierter Kontaktpersonen zu verhindern.

Die Datenschutzbehörde hatte sich infolge einer Beschwerde mit der medial kolportierten Pflicht zur Erhebung von Gästedaten durch GastronomInnen auseinanderzusetzen und kam zum Ergebnis, dass die Wiener Contact Tracing VO keine gesetzliche Verpflichtung zur Erhebung personenbezogener Daten normierte.

Der Beschwerdeführer hatte beim Betreten der Betriebsstätte eines Gastronomiebetriebes seinen Vor- und Nachnamen sowie seine Telefonnummer angegeben. Zur Erfassung der Daten ihrer KundInnen hatte die Gastronomin die Möglichkeit eingerichtet, sich online mittels QR-Code, der über das Mobiltelefon gescannt wurde, oder mittels Papierformular zu registrieren, wobei der Beschwerdeführer die Online Variante nutzte.

Die Beschwerdegegnerin berief sich darauf, gesetzlich zur Erhebung der Daten ihrer KundInnen verpflichtet zu sein und verwies in diesem Kontext auf § 5 Abs. 3 EpiG und die darauf gestützte Verordnung des Magistrats der Stadt Wien, insbesondere auf § 1 Z 2 lit. e leg. cit. Kein Zweifel bestand daran, dass es sich bei Vor- und Nachname sowie Telefonnummer um personenbezogene Daten des Beschwerdeführers handelte.

Die DSB hatte sich damit auseinanderzusetzen, ob diese Daten im gegenständlichen Fall auch als Gesundheitsdaten iSd Art. 4 Z 15 DSGVO zu betrachten waren. Die Datenschutzbehörde kam im Lichte der Rsp des EuGHs (C101/01 Rz 50) sowie in Fortschreibung ihrer ständigen Spruchpraxis, wonach aus Gesundheitsdaten jedenfalls Informationen über den früheren, gegenwärtigen oder künftigen körperlichen oder geistigen Gesundheitszustand der Betroffenen hervorgehen müssen, zum Ergebnis, dass in der gegenständlichen Konstellation auch Name und Telefonnummer als Gesundheitsdaten iSd Art. 4 Z 15 DSGVO zu qualifizieren waren. Dies ergab sich für die DSB daraus, dass die genannten Daten im Zusammenhang mit der Kontaktnachverfolgung zur Eindämmung potentieller Corona-Cluster nicht in ihrer gewöhnlichen Eigenschaft als bloßer Identifikator, sondern ausschließlich in einem gesundheitsbezogenen Kontext, verarbeitet wurden. Unter Berücksichtigung dieser Erwägungen war zu prüfen, ob die Verarbeitung unter den Voraussetzungen des Art. 9 Abs. 2 DSGVO zulässig gewesen ist.

Die Restaurantbetreiberin berief sich einerseits darauf, dass der Beschwerdeführer seine Daten freiwillig zur Verfügung gestellt habe, andererseits sei sie gesetzlich zur Verarbeitung der Daten verpflichtet gewesen. Festzuhalten ist, dass die Restaurantbetreiberin in ihrer Datenschutzerklärung einen Passus eingefügt hatte, wonach sie Kunden, die die Angabe ihrer Daten verweigern, unter Ausübung ihres Hausrechts des Lokales verweisen könnte.

Nach Auffassung der Datenschutzbehörde war unter diesen Umständen sowie mit Blick auf die Judikatur des EuGH (C-61/19 mwN) von keiner ausdrücklich erteilten Einwilligung iSd Art. 9 Abs. 2 lit. a DSGVO auszugehen, zumal dem Beschwerdeführer für den Fall, dass er sich geweigert hätte seine Daten zur Verfügung zu stellen, ein Nachteil in Form eines Lokalverweises

drohte. Es stand diesem jedoch auch keine zumutbare Alternative zur Verfügung, da andere Betriebstätten im Wiener Gemeindegebiet ebenso von der Verordnung erfasst waren und diese mit an Sicherheit grenzender Wahrscheinlichkeit gleichermaßen seine Daten erhoben hätten.

Somit stellte sich die Frage, ob dem Epidemiegesetz bzw. der darauf gestützten Durchführungsverordnung des Magistrats der Stadt Wien, eine gesetzliche Verpflichtung zur Verarbeitung personenbezogener Daten iSd Art. 9 Abs. 2 lit. i DSGVO zu entnehmen war.

Nach § 5 Abs. 3 EpiG sind alle Personen, die zu den Erhebungen über das Auftreten einer Krankheit einen Beitrag leisten können, auf Verlangen der Bezirksverwaltungsbehörde zur Auskunft verpflichtet. Diese Auskunftspflicht wurde durch die Wiener Contact Tracing Verordnung präzisiert, indem mittels Aufzählung klargestellt wurde, wer zur Auskunft gegenüber der Bezirksverwaltungsbehörde verpflichtet war und welchen Inhalt eine solche Auskunft zu enthalten hatte. Aus dem Umstand, dass eine Verletzung dieser Auskunftspflicht verwaltungsstrafrechtlich bewehrtes Verhalten darstellt, konnte keine Verpflichtung zur Erhebung von Kontaktdaten abgeleitet werden, zumal sich die Auskunftspflicht nur auf bereits vorhandene Daten erstreckte.

Die Verordnung war also hinsichtlich der Erhebung von Kontaktdaten nicht durch § 5 Abs. 3 EpiG gedeckt. Weiters genügte § 5 Abs. 3 EpiG iVm der Wiener Contact-Tracing Verordnung auch nicht den Anforderungen an eine Eingriffsnorm, da sie weder klare noch präzise Regeln für die Tragweite des Eingriffes in das Grundrecht auf Datenschutz erkennen ließen und somit dem Transparenzgebot im Sinne des Art. 5 Abs. 1 lit. a DSGVO nicht entsprachen. In Hinblick auf den Vorrang des Unionsrechts hatten diese Bestimmungen daher unangewendet zu bleiben. Die irreführende Vorgehensweise der Beschwerdegegnerin, sich zwar auf eine gesetzliche Verpflichtung zur Verarbeitung zu berufen, diese jedoch gleichzeitig von der freiwilligen Angabe der Daten durch ihre KundInnen abhängig zu machen, verletzte überdies den Grundsatz von Treu und Glauben.

Abschließend ist festzuhalten, dass die Verordnung des Magistrats der Stadt Wien betreffend Auskunftserteilung für Contact Tracing im Zusammenhang mit Verdachtsfällen von COVID-19 mit 31. Dezember 2020 außer Kraft getreten ist und das Epidemiegesetz zwischenzeitlich novelliert wurde. So wurde nunmehr in § 5c EpiG eine ausdrückliche gesetzliche Verpflichtung zur Erhebung von Kontaktdaten für Betreiber von Gastronomiebetrieben normiert, die mit 19.12. 2020 in Kraft getreten ist.

Dieser Bescheid ist rechtskräftig.

27. Bescheid vom 23.11.2020, GZ: 2020-0.586.738 (Datenverarbeitung im Rahmen des Zentralen Informationssystems „ZIS“)

Im gegenständlichen Fall hatte sich die Datenschutzbehörde unter anderem mit der Frage zu befassen, ob die Verarbeitung von Daten, konkret des Namens, Geburtsdatums sowie Umstands der Ablehnung eines Antrages auf Abschluss einer Lebensversicherung, im Rahmen des ZIS, eine Verletzung im Recht auf Geheimhaltung gemäß § 1 DSG darstellt.

Mangels qualifizierter gesetzlicher Grundlage für die gegenständliche Datenverarbeitung führte die Datenschutzbehörde eine Interessensabwägung durch, welche zugunsten des Versicherungsunternehmens ausfiel: Das ZIS stellt ein System zum wechselseitigen Informationsaustausch zwischen Versicherungsunternehmen dar und dient dem berechtigten Interesse dieser. Eine Einmeldung in das ZIS bewirkt zudem nicht zwingend eine anschließende Ablehnung eines Versicherungsvertrages und wurde gegenständlich eine solche Ablehnung als Folge der Eintragung auch nicht vorgebracht, sondern von der Beschwerdeführerin lediglich befürchtet.

Im Ergebnis lag daher eine rechtmäßige Datenverarbeitung vor und war die Beschwerde abzuweisen.

Dieser Bescheid ist rechtskräftig.

28. Bescheid vom 27.11.2020, GZ: 2020-0.620.698 (Veröffentlichung eines Wahlkampf-Veranstaltungs-Interviews auf Youtube rechtmäßig)

Die beiden Beschwerdegegner betrieben - als Hobby - einen Youtube-Kanal. Im Rahmen dieses Kanals veröffentlichten diese im September 2015 ein Video von einer Wahlkampfveranstaltung der FPÖ, auf der sie Personen zu politischen Themen wie „Asyl" bzw. „Ausländer" in einem Interview-Setting befragt hatten. Auch die Beschwerdeführerin war von den Beschwerdegegnern interviewt worden. Sie brachte bei der Datenschutzbehörde eine Beschwerde wegen Verletzung ihres Rechts auf Geheimhaltung ein, da sie der Veröffentlichung nicht zugestimmt habe.

Die Datenschutzbehörde wies die Beschwerde ab. Sie führte aus, dass es sich bei dem auf Youtube veröffentlichten Video, in dem die Beschwerdeführerin über die Themen „Asyl" bzw. „Ausländer" sprach, um die Verarbeitung von sensiblen Daten handelt, da dadurch ihre politische Meinung bzw. weltanschauliche Überzeugung ableitbar war. Weil die Beschwerdeführerin aktiv und freiwillig in ein Interview mit den Beschwerdegegnern eingewilligt hatte, entschied die Datenschutzbehörde, dass die Beschwerdeführerin ihre Daten im Sinn des Art. 9 Abs. 2 lit e DSGVO „offensichtlich öffentlich gemacht" gemacht hat. Somit war die Verarbeitung der Daten – hier: die Veröffentlichung des Videos auf Youtube – rechtmäßig. Die Datenschutzbehörde sprach auch aus, dass eine Interessenabwägung zwischen den Geheimhaltungsinteressen der Beschwerdeführerin und dem Interesse der Beschwerdegegner an einer freien Meinungsäußerung ebenfalls zum Ergebnis führt, dass die Verarbeitung erlaubt ist. Dies, weil die Interessen der Beschwerdegegner stärker wiegen.

Dieser Bescheid ist rechtskräftig.

Österreichische Post AG

Mit mehreren Millionen verarbeiteten Datensätzen zählt die Österreichische Post AG mittlerweile zu den führenden Direktmarketingunternehmen in Österreich. Im Rahmen dieser Tätigkeit verarbeitete die Österreichische Post AG unter anderem die „Parteiaffinitäten". Inhalt dieses Datensatzes sind Wahrscheinlichkeitswerte, mit denen eine Person einer politischen Partei „zugeneigt" ist. Aufgrund zahlreicher Medienberichte und damit einhergehend sprunghaftem Anstieg der Beschwerden gegen die Österreichische Post AG stand der Verdacht des systematischen Verstoßes gegen datenschutzrechtliche Pflichten im Raum. In der Folge wurde zu Beginn des Jahres 2019 ein amtswegiges Prüfverfahren gegen die Österreichische Post betreffend „Parteiaffinitäten" eingeleitet (siehe Bescheid vom 11. Februar 2019, GZ: D2013.747/0002-DSB/2019). Datenschutzrechtliche Beschwerdeverfahren gegen die Österreichische Post AG werden aufgrund der hohen Fallzahlen seit Herbst 2019 von einer eigens dafür eingerichteten Task-Force geführt.

Im Berichtszeitraum wurden 205 Neueingaben protokolliert. 173 Verfahren wurden einer Enderledigung zugeführt. Die Arbeit der Post-Task-Force zeichnet sich durch die Fortentwicklung der datenschutzrechtlichen Spruchpraxis im Rahmen von Auskunfts- und Geheimhaltungsbeschwerden aus.

Wesentliche Entscheidungen:

1. Bescheid vom 24.6.2020, GZ: 2020-0.140.595 (qualifizierte elektronische Signatur als ausreichender Identitätsnachweis) und Bescheid vom 9.7.2020, GZ: 2020-

0.033.062 (keine routinemäßige Identitätsprüfung nach der DSGVO), beide nicht rechtskräftig

Im Zusammenhang mit den antragsbedürftigen Betroffenenrechten nach der DSGVO hatte sich die DSB in zwei ähnlich gelagerten Fällen mit der Frage des ausreichenden Identitätsnachweises auseinanderzusetzen. Dabei wurde den Beschwerden wegen Verletzung im Recht auf Auskunft stattgegeben und der systematischen Identitätsüberprüfung im Ergebnis eine Absage erteilt.

Begründend wurde insbesondere auf die veränderte Rechtslage seit dem In Geltung treten der DSGVO hingewiesen, nach deren ausdrücklichem Gesetzeswortlaut ein Identitätsnachweis nur bei Vorliegen begründeter Zweifel und nur nach Vornahme einer einzelfallbezogenen Prüfung zulässig ist. Zudem wurde festgehalten, dass es sich bei der qualifizierten elektronischen Signatur nach dem SigG um einen ausreichenden Identitätsnachweis handelt.

Beide Bescheide sind nicht rechtskräftig.

2. Bescheid vom 24.9.2020, GZ: 2020-0.542.231 (rechtswidrige Verarbeitung der „Sinus-Geo-Milieus", nicht rechtskräftig)

Mit Teilerkenntnis vom 20. August 2020 (GZ: W258 2217446-1/15E) bestätigte das Bundesverwaltungsgericht die Rechtsansicht der DSB betreffend die rechtswidrige Verarbeitung der „Parteiaffinitäten".

Im Lichte dieses Erkenntnisses stellte die DSB in Folge fest, dass die Verarbeitung der „Sinus-Geo-Milieus" als Verarbeitung besonderer Kategorien personenbezogener Daten (konkret: Weltanschauung) zu qualifizieren ist, die sich mangels (ausreichend determinierter) Rechtsgrundlage als rechtswidrig darstellte. Der diesbezüglichen Beschwerde gegen die Österreichische Post AG wegen Verletzung im Recht auf Geheimhaltung wurde daher stattgegeben.

Die DSB führte in der Bescheidbegründung aus, dass es sich bei statistisch errechneten Daten dann um sensible personenbezogene Daten handelt, wenn diese einer individuellen Person zugeordnet und folglich qualifiziert verknüpft werden. In Anbetracht des Schutzzweckes des Art. 9 DSGVO ist es hingegen irrelevant, ob die Wahrscheinlichkeitswerte tatsächlich richtig oder objektiv nachprüfbar sind. Abschließend wurde erneut festgehalten, dass die GewO 1994 mangels erheblichem öffentlichen Interesses keine qualifizierte Rechtsgrundlage darstellt.

Dieser Bescheid ist nicht rechtskräftig.

3. Bescheid vom 17.12.2020, GZ: 2020-0.822.464 (keine parallele oder sukzessive Verfahrensführung vor Zivilgerichten und Aufsichtsbehörden, nicht rechtskräftig)

In diesem Bescheid hatte sich die DSB mit den Grenzen der Parallelzuständigkeit zwischen den ordentlichen Gerichten und Aufsichtsbehörden auseinanderzusetzen. Der Beschwerdeführer hatte bereits vor Erhebung der Beschwerde bei der DSB den zivilrechtlichen Weg beschritten, worüber auch bereits rechtskräftig entschieden worden war. Die Beschwerde wegen Verletzung im Recht auf Auskunft wurde folglich wegen Identität der Sache zurückgewiesen.

Die DSB hielt dazu begründend fest, dass eine parallele oder sukzessive Verfahrensführung vor den Zivilgerichten und den Aufsichtsbehörden die Gefahr einander widersprechender Entscheidungen impliziert. Obgleich Art. 79 DSGVO unbestrittenermaßen betroffenen Personen die Wahl des Rechtsweges – zwischen ordentlichem Gericht und verwaltungsbehördlichem Verfahren – garantiert, wäre es zweckwidrig, zunächst ein Gericht mit der Frage der Rechtmäßigkeit zu befassen, nur um dieselbe Frage nach Abschluss des Rechtszuges der Beantwortung

durch eine Aufsichtsbehörde zuzuführen. Mangels Rechtsschutzbedürfnisses blieb daher kein Raum für eine erneute Überprüfung durch die DSB.

Dieser Bescheid ist nicht rechtskräftig.

3.2.1.2 Grenzüberschreitende Fälle der DSB[2]

Im Jahr 2020 wurden bei der DSB 219 Beschwerdefälle eingebracht, die einen grenzüberschreitenden Sachverhalt iSd Art. 4 Z 23 DSGVO aufwiesen.

Die DSB war seit 25. Mai 2018 bis Ende 2020 in 29 Verfahren als federführende Aufsichtsbehörde gegenüber einem Verantwortlichen tätig, wobei den anderen betroffenen Aufsichtsbehörden iSd Art. 4 Z 22 DSGVO seitens der DSB im Jahr 2020 in 3 Verfahren ein Beschlussentwurf gemäß Art. 60 Abs. 3 DSGVO vorgelegt wurde.

Zwei dieser Verfahren betrafen Verletzungen im Recht auf Auskunft gemäß Art. 15 DSGVO bzw. Löschung gemäß Art. 17 DSGVO, die im laufenden Verfahren beseitigt wurden. Der dritte Beschwerdefall, wegen einer Verletzung im Recht auf Auskunft gemäß Art. 15 DSGVO sowie einer Verletzung im Recht auf Widerspruch gemäß Art. 21 DSGVO, wurde, mangels Antragstellung an die Verantwortliche vor Beschwerdeerhebung, abgewiesen.

Im Rahmen der grenzüberschreitenden Zusammenarbeit innerhalb und außerhalb eines konkreten Verfahrens machte die DSB 2020 65 Mal von der gegenseitigen Amtshilfe iSd Art. 61 DSGVO Gebrauch und wurde selbst in 242 Fällen von anderen Aufsichtsbehörden kontaktiert.

Insgesamt wurden seit dem 25. Mai 2018 bis Ende 2020 von allen Aufsichtsbehörden 173 Beschlussentwürfe iSd Art. 60 Abs. 3 DSGVO vorgelegt, die in 168 finalen Beschlüssen iSd Art. 60 Abs. 6 DSGVO mündeten.

Ein grenzüberschreitendes Verfahren mündete 2020 in einer Streitbeilegung iSd Art. 65 Abs. 1 lit. a DSGVO vor dem EDSA:

Gegen den Beschlussentwurf der irischen Datenschutzbehörde, im Rahmen eines amtswegigen Prüfverfahrens wegen eines data breaches der Twitter International Company wurden zahlreiche Einsprüche, unter anderem auch von der österreichischen Datenschutzbehörde, erhoben, die in weiterer Folge von der irischen Datenschutzbehörde als nicht maßgeblich oder als unbegründet zurückgewiesen wurden, weshalb es zur Einleitung des Streitbeilegungsverfahrens iSv Art. 65 Abs. 1 lit. a DSGVO kam.

Der Europäische Datenschutzausschuss überprüfte im Rahmen des Streitbeilegungsverfahrens zunächst, welche Einsprüche iS des Art. 4 Z 24 DSGVO die definitionsgemäßen Maßstäbe erfüllten. Hierbei mussten bereits einige der Einsprüche aufgrund des Nichtvorliegens der Voraussetzungen des Art. 4 Z 24 DSGVO abgewiesen werden.

Im Hinblick auf die Einsprüche betreffend Wirksamkeit, Verhältnismäßigkeit und Abschreckung iS des Art. 83 Abs. 1 DSGVO sprach der der Europäische Datenschutzausschuss in seiner ersten Entscheidung [3] gemäß Art. 65 Abs. 1 lit. a DSGVO vom 9. November 2020 mit Zweidrittelmehrheit aus, dass die irische Aufsichtsbehörde eine Neubewertung der Strafhöhe (im Sinne einer

2 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.

3 Die Entscheidung des EDSA ist unter folgendem Link abrufbar: https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/decision-012020-dispute-arisen-draft_de

Erhöhung) unter Heranziehung der (Erschwernis)gründe von Art. 83 Abs. 2 DSGVO durchzuführen habe.

Mit Entscheidung vom 9. Dezember 2020 setzte die irische Datenschutzbehörde die Entscheidung des Europäischen Datenschutzausschusses um[4] und setzte die Geldbuße mit $ 500.000,-- (umgerechnet ca. € 450.000,--) fest.

Darüber hinaus obliegt der DSB auch die Zuständigkeit zur Verfahrensführung 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.

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. Im Berichtszeitraum wurden 3227 schriftliche Rechtsauskünfte erteilt. 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

Die DSGVO brachte als eine wesentliche Änderung die weitgehende Genehmigungsfreiheit für den internationalen Datenverkehr an Empfänger außerhalb des EWR.

Die DSGVO regelt die Übermittlung personenbezogener Daten an Empfänger in Drittländern oder in internationalen Organisationen in ihrem Kapitel V und sieht hierzu unterschiedliche rechtliche Instrumente vor. Grundsätzlich ist eine Genehmigung dieser Instrumente durch die zuständige Aufsichtsbehörde nur mehr in bestimmten Fällen gemäß Art. 46 Abs. 3 DSGVO vorgesehen.

Eine weitere Ausnahme bilden etwa die nunmehr ausdrücklich in der DSGVO verankerten „Verbindlichen internen Datenschutzvorschriften“ (Binding Corporate Rules – BCRs), welche von der zuständigen Aufsichtsbehörde unter Anwendung des Kohärenzverfahrens gemäß Art. 63 ff DSGVO genehmigt werden. Hierbei ist eine enge Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss notwendig.[5] Die in

4 final_decision_-_in-19-1-1_9.12.2020.pdf (europa.eu)

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

einem ersten Schritt zu bestimmende federführende Aufsichtsbehörde übernimmt dabei die Kommunikation mit dem Antragsteller, hat aber gleichzeitig die Kommentare und Anmerkungen aller anderen Aufsichtsbehörden zu berücksichtigen. Der finale Entwurf muss dem Europäischen Datenschutzausschuss vorgelegt werden, welcher über die Annahme des Entwurfs abstimmt.

Aufgrund des zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss vorgesehenen Abstimmungsprozesses sowie des generell für alle Beteiligten aufwendigen Verfahrens kann sich die Behandlung derartiger Anträge bis zur endgültigen Genehmigung von BCRs über einen langen Zeitraum erstrecken.

Aufgrund ihrer Komplexität sollte daher im ersten Schritt immer nach der Notwendigkeit von BCRs gefragt werden. Insbesondere sollte abgewogen werden, ob die Zulässigkeit der Datenübermittlung an Empfänger außerhalb des EWR 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 Drittländern gering ist. BCRs sollten immer nur dann zum Einsatz kommen, wenn die Nutzung anderer geeigneter Garantien problematisch erscheint.[6]

Bei der Datenschutzbehörde wurden im Jahr 2020 zwei neue BCR-Genehmigungsverfahren anhängig gemacht.

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 2020

Die Datenschutzbehörde hat im Jahr 2020 20 Bescheide im Rahmen der §§ 7,8 DSG erlassen, davon fünf Zurückweisungen (wg. der Erfüllung der Voraussetzung des § 7 Abs. 1 Z 1 DSG [*„öffentlich zugängliche Daten“*], des § 7 Abs. Z 3 DSG [*„für den Verantwortlichen pseudonymisierte personenbezogene Daten“*], wg. § 13 Abs. 3 AVG [nicht beantworteter Mangelbehebungsauftrag], wg. mangelnder Verantwortlicheneigenschaft iSd § 8 Abs. 4 DSG sowie wg. Vorliegens der Genehmigungsfreiheit iSd § 8 Abs. 2 Z 1 DSG [*„Beeinträchtigung der Geheimhaltungsinteressen unwahrscheinlich und Verarbeitung der Daten durch denselben Verantwortlichen“*]).

11 Entscheidungen betrafen erteilte Genehmigungen gemäß § 7 DSG zu Forschungszwecken. Davon kann ein großer Teil direkt oder indirekt dem Straßenverkehr zugeordnet werden (etwa Forschungen betreffend die automationsunterstützte Verkehrskonfliktanalyse, die automationsunterstützte Analyse von Verkehrssicherheitseinrichtungen, die Entwicklung von

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

Assistenzfunktionen und (teil)autonomen Systemen sowie betreffend automatisierter Kleinbusse im öffentlichen Personennahverkehr).

Von allgemeinem Interesse erscheint der Bescheid vom 21. Jänner 2020 zur GZ D202.235 (2020-0.013.649), mit dem über den Antrag einer außeruniversitären Forschungseinrichtung für eine Datenverarbeitung, zum Zweck der Erarbeitung von Testdaten für Algorithmen im Bereich des (teil)autonomen Fahrens personenbezogene Daten im Zuge von Bildaufnahmen an öffentlichen Orten innerhalb Österreichs bzw. der Europäischen Union aus Sicht des Fahrers von Straßen bzw. Schienenfahrzeugen zu ermitteln und zu verarbeiten, abgesprochen worden ist. Während der Antrag betreffend die Datenverarbeitung des Projekts innerhalb Österreichs aufgrund des Vorliegens der Voraussetzungen des § 7 Abs. 3 DSG genehmigt wurde, wurde dieser hinsichtlich des übrigen Unionsbereiches zurückgewiesen. Begründend wird ausgeführt, dass bei der Verarbeitung von personenbezogenen Daten zu Forschungszwecken nicht nur Bedacht auf die Regelungen der DSGVO zu nehmen ist, sondern auch auf die jeweiligen nationalen Vorschriften, die die (fakultative) Öffnungsklausel des Art. 6 Abs. 2 iVm Art. 89 DSGVO umsetzen (Stichwort: „hinkende Verordnung"). Darüber hinaus wird darauf hingewiesen, dass der österreichischen Datenschutzbehörde gem. Art. 55 Abs. 1 DSGVO nur im eigenen Staatsgebiet Jurisdiktionskompetenz zukommt und dies somit einer Genehmigung für die gesamte Europäische Union entgegensteht.

Abschließend hervorzuheben ist der Bescheid vom 01. Oktober 2020 zur GZ D202.254 (2020-0.558.824), der die Durchführung einer populationsbasierten Beobachtungsstudie genehmigt, die sich mit dem Outcome (=Behandlungsergebnis) von Notarzteinsätzen betreffend Kinder und Jugendliche innerhalb eines mehrjährigen Zeitraumes in einem Bundesland beschäftigt. Im Rahmen dieser Studie werden die Gesundheitsdaten dieser vulnerablen betroffenen Personen ermittelt und verarbeitet. Insbesondere ist zu erwähnen, dass in diesem Fall das Vorliegen eines wichtigen öffentlichen Interesses gem. § 7 Abs. 3 zweiter Unterabsatz DSG Voraussetzung für die Genehmigung war, da im Rahmen des Forschungsprojektes besondere Datenkategorien iSd Art. 9 DSGVO verarbeitet werden. Das wichtige öffentliche Interesse hat sich aus dem Zweck des Forschungsprojektes – der Verbesserung der präklinischen Versorgung der genannten Personengruppe – zweifellos ergeben.

3.2.5 Amtswegige Prüfverfahren

Die DSB hat im Jahr 2020 337 amtswegige Verfahren eingeleitet; 154 amtswegige Verfahren wurden im Berichtszeitraum einer Enderledigung (Bescheid oder Einstellung) zugeführt.

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 2020 wurde – bedingt durch die anhaltend hohe Belastung nach in Geltungtreten der DSGVO und dem damit verbundenen generellen Anstieg an Verfahrenszahlen – wie im davorliegenden Berichtszeitraum kein Schwerpunktverfahren durchgeführt.

Ausgewählte Entscheidungen:

1. Lehrerbewertungsplattform „Lernsieg", DSB-D213.953

Im Rahmen dieses amtswegigen Prüfverfahrens zog die Datenschutzbehörde die datenschutzrechtliche Zulässigkeit der App „Lernsieg" (Bewertungsplattform, auf der Schüler ihre eigenen Schulen und Lehrer in einem Punktesystem bewerten können) in Prüfung. Als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten von Lehrern und der zu ihnen bestehenden Wertungen dient Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen): Die Verarbeitung der Daten beruht auf dem Recht auf freie Meinungsäußerung und Information. Es soll eine verstärkte Transparenz im Bereich der Bildung erreicht werden und die Qualität der Ausbildung im Unterricht einer nachvollziehbaren Kontrolle zugänglich sein.

Im Rahmen der aus Art. 6 Abs. 1 lit. f DSGVO erfließenden Pflicht zur Abwägung der Interessen stand insbesondere die Verwendung der App, um anonym Meinungen und Werturteile äußern zu können, dem Interesse von Lehrern gegenüber, dass das eingeschränkt öffentliche Handeln vor einer Klasse im Rahmen der dienstlichen Berufsausübung nicht einer breiten Öffentlichkeit, die die abgegebenen Bewertungen inhaltlich nicht verifizieren oder falsifizieren kann, zugänglich gemacht wird. Besonderes Augenmerk war daher darauf zu legen, dass einerseits die Anprangerung von betroffenem Lehrpersonal in potentiell unbegrenzter Öffentlichkeit keinem entsprechenden individuellen Nutzen entgegensteht, obgleich Bewertungsplattformen Vergleichbarkeit und Transparenz fördern. Eine Besonderheit der Bewertungsplattform „Lernsieg" liegt darin, dass die Bewertung nur in Form von zu vergebenden Sternen erfolgen kann, dass nur vordefinierte Kommentare ausgewählt werden können und dass kein Freitextfeld für Kommentare zur Verfügung steht.

Vor diesem Hintergrund gelangte die Datenschutzbehörde zu dem Ergebnis, dass die Interessenabwägung zugunsten einer Zulässigkeit der Datenverarbeitung in Form der Bewertungsplattform „Lernsieg" ausgeht.

Der Bescheid ist rechtskräftig.

2. Informationspflichten und „irrtümliches Profiling", DSB-D213.1068

Die Datenschutzbehörde prüfte die Richtigkeit der Informationen gemäß Art. 13 DSGVO, die im Einwilligungsformular in die Datenverarbeitung eines Finanzinstituts erteilt wurden:
Der Verantwortliche führte in seiner Datenschutzerklärung aus, dass er personenbezogene Daten aus sozialen Netzwerken von betroffenen Person auswerte, um die Zusendung personalisierter Werbung zu ermöglichen. Es ergab sich jedoch, dass das dafür erforderliche „Profiling" gar nicht vorgenommen wurde und diese Information nur „aus Vorsichtsgründen" in die Datenschutzerklärung aufgenommen wurden.

Die Datenschutzbehörde hat dazu ausgesprochen, dass der Zweck der Informationen gemäß Art. 13 DSGVO (auch) darin besteht, über den Umstand der Verarbeitung von Daten aufzuklären, um die Geltendmachung von Rechten zu ermöglichen. Der Verweis auf die nicht existente Datenverarbeitung „Profiling" konterkariert das Transparenzgebot und widerspricht den Vorgaben von Art. 12 Abs. 1 sowie der Informationspflicht gemäß Art. 13 Abs. 1 lit. c DSGVO.

Dieser Bescheid ist rechtskräftig.

3. „AMS-Algorithmus", DSB-D213.1020

In diesem Verfahren setzte sich die Datenschutzbehörde mit der Zulässigkeit der Verwendung eines Assistenz-Systems (in Folge: „AMAS") zur Auswahl von Maßnahmen bei Arbeitssuchenden

auseinander. Bei AMAS handelt es sich um einen eigens programmierten Algorithmus, der anhand der zur einer bestimmten Person gespeicherten Faktoren, wie Altersgruppe, Geschlecht, Staatengruppe, Ausbildung, gesundheitliche Beeinträchtigungen, Betreuungspflichten, Berufsgruppe, Vorkarriere, regionales Arbeitsmarktgeschehen und Dauer des Geschäftsfalls beim AMS, die Chance errechnet, in Zukunft für einen bestimmten Zeitraum wieder beschäftigt zu sein, berechnet. Die berechneten Wahrscheinlichkeiten können von Mitarbeitern verwendet werden, um passende Maßnahmen mit Arbeitssuchenden zu vereinbaren bzw. zu setzen (etwa Weiterbildungsmöglichkeiten).

Die entscheidende Frage war, ob diese Datenverarbeitung auf §§ 25 Abs. 1, 29 und 31 Abs. 5 AMSG sohin auf eine gesetzliche Grundlage gestützt werden kann.

Die DSB wertete diese Form der Datenverarbeitung als Profiling iSd Art. 4 Z 4 DSGVO, weshalb sie Art. 22 DSGVO als einschlägig erachtete.

Da es sich beim AMS um eine staatliche Behörde handelt, ist für diese Form der Datenverarbeitung eine hinreichend klare Gesetzesgrundlage erforderlich.

Die DSB konnte eine solche im AMSG nicht erblicken und wertete die vom AMS verabschiedete „Bundesleitlinie" zur Handhabung von AMAS (darin ist insbesondere geregelt, dass trotz errechnetem Ergebnis ein persönliches Gespräch zu führen ist) als nicht ausreichende Rechtsgrundlage, weil diese gegenüber Dritten – wie Arbeitssuchenden – keine Rechtswirkung entfalten kann.

Die Datenschutzbehörde entschied daher, dass die Verwendung von AMAS wegen exzessiven Umfangs und weitreichender Wirkung der Verarbeitung nicht hinreichend von einer Rechtsgrundlage gedeckt ist. Die Datenverarbeitung wurde daher im gegebenen Umfang untersagt, und die aufschiebende Wirkung einer Bescheidbeschwerde ausgeschlossen.

Im Rechtsmittelverfahren vor dem BVwG wurde mittlerweile ausgesprochen, dass nach Ansicht des BVwG § 25 AMSG eine ausreichende Rechtsgrundlage für die hier relevante Datenverarbeitung darstellt.

Die Datenschutzbehörde hat Amtsrevision an den VwGH erhoben.

3.2.6 Beschwerdeverfahren vor dem Bundesverwaltungsgericht einschließlich Säumnisbeschwerden

Im Jahr 2020 wurden 319 Beschwerden gegen Bescheide der Datenschutzbehörde erhoben.

Es gab 45 Säumnisbeschwerden im Berichtszeitraum.

W274 2228071-1/6E, Erkenntnis vom 29. April 2020

Mit diesem Erkenntnis bestätigte das Bundesverwaltungsgericht, dass die Datenschutzbehörde die Behandlung einer Beschwerde wegen „Exzessivität" zurecht abgelehnt hat.

Die Datenschutzbehörde ist zwar verpflichtet, sich mit Beschwerden gemäß Art. 57 Abs. 1 lit. f DSGVO zu befassen, kann die Behandlung einer Beschwerde aber ablehnen, wenn die Beschwerdeerhebung offenkundig unbegründet oder – insbesondere im Fall von häufiger Wiederholung – exzessiv erfolgt (Art. 57 Abs. 4 DSGVO).

Ablehnung bedeutet diesfalls, dass die DSB keine inhaltliche Beurteilung der Beschwerde vornimmt, sondern die Behandlung vor einer solchen Prüfung ablehnt. Im vorliegenden Fall brachte der Beschwerdeführer seit Juni 2018 mehr als 90 Beschwerden (zum Zeitpunkt der Erlassung des Bescheides der Datenschutzbehörde) ein, die sich im Kern um dieselbe Sache drehten, nämlich darum, dass der Beschwerdeführer verschiedenen Verantwortlichen (in Österreich und einem anderen Staat der EU) vorwarf, seine Daten und die Daten seines Kindes unrichtig bzw. unrechtmäßig zu verarbeiten.

Das Bundesverwaltungsgericht hielt im genannten Erkenntnis fest, dass die Ablehnung wegen exzessiver Verfahrensführung zurecht erfolgte und hielt begründend fest: „Der Beschwerdeführer zeigt in seiner Beschwerde an das BVwG nicht auf, dass der der Datenschutzbeschwerde zugrundeliegende Sachverhalt […] so individuell wäre, dass trotz der hohen Anzahl von Beschwerden generell als auch den mehreren Beschwerden gegen Beschwerdegegner im Zusammenhang mit [Einrichtung] eine Behandlung der Beschwerde berechtigt wäre."

Dieses Erkenntnis ist rechtskräftig.

W214 2228346-1, Erkenntnis vom 27. Mai 2020

Die Mit Bescheid vom 5. Dezember 2019, GZ: DSB-D124.630/0004-DSB/2019 gab die Datenschutzbehörde einer Beschwerde wegen Verletzung im Recht auf Auskunft statt und trug dem Beschwerdegegner (ein Verantwortlicher des öffentlichen Bereichs) auf, dem Antrag auf Auskunft des Beschwerdeführers zu entsprechen, da dieser sich entgegen den Ausführungen des Beschwerdegegners ausreichend identifiziert hat.

Das Auskunftsbegehren wurde mit einer qualifizierten elektronischen Signatur versehen und kam die Datenschutzbehörde zum Schluss, dass der Beschwerdeführer seine Identität ausreichend nachgewiesen hat. Dies auch angesichts der Tatsache, dass der Beschwerdeführer darüber hinaus seine aktuelle sowie seine ehemalige Adresse und seine E-Mail-Adresse im Auskunftsbegehren angeführt hat. Dahingegen hat es der Beschwerdegegner verabsäumt darzulegen, aus welchen Gründen er Zweifel an der Identität des Beschwerdeführers hat.

Die Datenschutzbehörde trug dem Beschwerdegegner auf, dem Auskunftsbegehren des Beschwerdeführers zu entsprechen. Dies unter Verweis darauf, dass die in § 24 Abs. 5 DSG normierte Einschränkung auf Verantwortliche des privaten Bereiches aufgrund des unmittelbaren Vorranges des Unionsrechts unangewendet zu bleiben hat.

Das Bundesverwaltungsgericht pflichtete der Datenschutzbehörde in seinem Erkenntnis bei, dass kein Grund ersichtlich ist, weshalb der Beschwerdegegner an der Identität zweifeln hätte können und teilte die Ansicht der Datenschutzbehörde, wonach die elektronische Signatur – im vorliegenden Fall – ein geeignetes Mittel zum Nachweis der Identität darstellt.

Des Weiteren bestätigte das Bundesverwaltungsgericht die Rechtsansicht der Datenschutzbehörde, wonach die Einschränkung des § 24 Abs. 5 DSG auf Verantwortliche des privaten Bereiches aufgrund des Anwendungsvorranges des Art. 58 Abs. 2 lit. c DSGVO, der eine solche Einschränkung nicht vorsehe, unangewendet zu bleiben hat.

Dieses Erkenntnis ist rechtskräftig.

W258 2217446-1/15E und W258 2217446-1/35E, Teilerkenntnisse vom 20. August 2020 und vom 26. November 2020 (Verarbeitung von „Parteiaffinitäten" durch die Österreichische Post AG)

Mit erstem Teilerkenntnis bestätigte das Bundesverwaltungsgericht teilweise einen Bescheid der Datenschutzbehörde, wonach es sich bei den Daten zur „Parteiaffinität“ um besondere Kategorien personenbezogener Daten iSd Art. 9 DSGVO handle, die dem darin normierten Verarbeitungsverbot unterliegen und demnach unrechtmäßig verarbeitet wurden.

Begründend führte das Bundesverwaltungsgericht zusammengefasst aus, der Unionsgesetzgeber habe in der Verwendung des Ausdrucks „alle Informationen“ das Ziel vor Augen gehabt, dem Begriff der „personenbezogenen Daten“ eine weite Bedeutung beizumessen. Weiters ergebe sich aus der „Parteiaffinität“ eine hinreichende Wahrscheinlichkeit des Hervorgehens der politischen Meinung, weshalb besondere Kategorien personenbezogener Daten iSd Art. 9 DSGVO vorliegen würden. Werden Personen mit einer hohen „Parteiaffinität“ für eine bestimmte politische Meinung empfänglich angesehen und sollen deshalb gezielt mit Werbung über politische Parteien beworben werden, würden dazu spiegelbildlich die Gefahren stehen, die Art 9 DSGVO vermeiden möchte.

Das Bundesverwaltungsgericht stellte sodann klar, dass § 151 Abs. 6 GewO 1994 keine Regelung iSd Art. 9 Abs 2 lit. g DSGVO sei, welche eine Verarbeitung besonderer Kategorien personenbezogener Daten zulässig machen würde. Man könne nämlich kein erhebliches öffentliches Interesse iSd Art. 9 Abs. 2 lit. g annehmen, wenn durch die Rechtsnorm lediglich die Tätigkeit eines bestimmten Wirtschaftsbereichs erleichtert werden soll. Die Allgemeinheit wäre in derartigen Fällen ohne die in Rede stehende Maßnahme regelmäßig nicht ernsthaft beeinträchtigt, weshalb die Verarbeitung der Datenarten zur „Parteiaffinität“ nicht auf Art. 9 Abs. 2 lit. g DSGVO iVm § 151 Abs 6 GewO 1994 gestützt werden könne.

Da sich die Österreichische Post AG auch auf keine der anderen Ausnahmebestimmungen des Art. 9 Abs. 2 DSGVO vom Verarbeitungsverbot besonderer Kategorien von Daten des Art. 9 Abs. 1 DSGVO berufen könne, insbesondere habe sie keine Zustimmung für die Verarbeitung von den Betroffenen eingeholt, erweise sich die Verarbeitung der Daten zur „Parteiaffinität“ als rechtswidrig.

Das Teilerkenntnis ist nicht rechtskräftig.

Gegenstand des zweiten Teilerkenntnisses waren die zwei Spruchpunkte des Bescheides der Datenschutzbehörde, in welchen der Österreichische Post AG aufgetragen wurde, die Parteiaffinitäten zu löschen, eine Verarbeitung derselben zu unterlassen sowie die Datenschutz-Folgenabschätzung und das Verarbeitungsverzeichnis entsprechend anzupassen.

Die Leistungsaufträge zur Löschung der Parteiaffinitäten und zur Anpassung der Datenschutz-Folgenabschätzung und des Verarbeitungsverzeichnisses wurden ersatzlos behoben, weil die Grundlage für die Erteilung dieser Aufträge weggefallen ist (keine Verarbeitung der „Parteiaffinitäten“ mehr durch die Österreichische Post AG).

In Bezug auf den Unterlassungsauftrag wurde die Beschwerde abgewiesen und der entsprechende Spruchpunkt leicht abgeändert.

Auch dieses Teilerkenntnis ist nicht rechtskräftig.

GZW211 2227144-1/3E, Erkenntnis vom 23. November 2020
Das Bundesverwaltungsgericht hat mit diesem Erkenntnis einer Beschwerde gegen den Bescheid der Datenschutzbehörde vom 18. September 2019, GZ: DSB-D124.522/0001-DSB/2019, stattgegeben.

Im Bescheid hat die Datenschutzbehörde eine Beschwerde wegen Verletzung im Recht auf Geheimhaltung zurückgewiesen, da Untersuchungsausschüsse und protokollarische Aufzeichnungen über Beweiserhebungen (§ 19 der Anlage 1 zum GOG-NR, VO-UA) Aufgaben der legislativen Kontrolle über die Verwaltung seien und folglich nicht der Jurisdiktionskompetenz der Datenschutzbehörde unterlägen.

Zur Prüfbefugnis der Datenschutzbehörde hat das Bundesverwaltungsgericht zusammengefasst im Wesentlichen ausgeführt, dass diese in der DSGVO grundsätzlich umfassend angelegt sei und die DSGVO selbst eine Zuständigkeit der Datenschutzbehörde für datenschutzrechtliche Vorgänge im Rahmen der Gesetzgebung nicht ausschließe. Ebenso kenne auch das DSG keine Bestimmung, nach der eine Kontrolle der Datenschutzbehörde über datenschutzrechtliche relevante Vorgänge bei Untersuchungsausschüssen ausgeschlossen sein könnte. Eine Ausnahme sei nur in § 31 Abs. 1 DSG hinsichtlich Gerichte im Rahmen ihrer justiziellen Tätigkeit vorgesehen. Es fehle an einer ausdrücklichen Rechtsgrundlage, die die Kontrollbefugnis der Datenschutzbehörde ausschließe. Der Umstand, dass Untersuchungsausschüsse in der Verfassungsbestimmung des § 35 Abs. 2 DSG nicht genannt sind, führe angesichts des Vorrangs von Unionsrecht nicht dazu, dass der Datenschutzbehörde keine Kontrollbefugnis zukomme. Zwar stelle die Sonderregel des Art. 55 Abs. 3 DSGVO offenkundig eine Ausnahme betreffend die justizielle Tätigkeit der Gerichte dar, jedoch ist diese einer Verallgemeinerung nicht zugänglich, sodass in weiterer Folge die Zuständigkeit der Aufsichtsbehörden auch hinsichtlich parlamentarischer Untersuchungsausschüsse zu bejahen sei.

Dieses Erkenntnis ist nicht rechtskräftig, es wurde seitens der Datenschutzbehörde mit Amtsrevision bekämpft.

W274 2225373-1/9E, Erkenntnis vom 4. Dezember 2020
Im Bescheid vom 1. August 2019, GZ: DSB-D123.382/0002-DSB/2019, gab die Datenschutzbehörde einer Beschwerde wegen Verletzung im Recht auf Geheimhaltung statt und stellte eine Rechtsverletzung dadurch fest, indem eine Staatsanwaltschaft im Zuge der Benachrichtigung von Betroffenen einer Telekommunikationsdatenerfassung diesen nicht nur die Anordnung bzw. Bewilligung dieser Erfassung, sondern auch die Begründung hiezu, welche personenbezogene Daten des Beschwerdeführers über vorgeworfene strafbare Handlungen enthält, übermittelt hat.

Mit dem Erkenntnis wurde der Beschwerde der Staatsanwaltschaft stattgegeben und der Bescheid dahingehend abgeändert, dass dessen Spruch zu lauten hat, dass die Beschwerde abgewiesen wird.

Das Bundesverwaltungsgericht führt begründend aus, dass nach den Materialien zum Materien-Datenschutz-Anpassungsgesetz 2018 (BGBl. I Nr. 32/2018) die einschlägigen materienspezifischen Regelungen zur Datenverarbeitung, wie jene der StPO, dem 3. Hauptstück des DSG vorgehen und die StPO einen „generalisierenden“ Vorrang gegenüber dem DSG habe.

Des Weiteren hielt das Bundesverwaltungsgericht in seiner rechtlichen Beurteilung fest, dass ein Betroffener einer Telekommunikationsdatenerfassung, um seine Rechtschutzmöglichkeiten ausüben zu können, ein Mindestmaß an Informationen auf Tatsachenebene benötige. Hierunter fallen auch Angaben zum Tatverdacht sowie Ausführungen, worauf sich dieser Tatverdacht gründet.

Dieses Erkenntnis ist nicht rechtskräftig, es wurde seitens der Datenschutzbehörde mit Amtsrevision bekämpft.

W274 2214412-1/5E, Erkenntnis vom 4. Dezember 2020
Im Bescheid vom 4. Jänner 2019, GZ: DSB-D123.264/0007-DSB/2018, wurde von der Datenschutzbehörde ausgesprochen, dass die zeitgleiche Inanspruchnahme des Beschwerderechts gemäß Art. 77 Abs. 1 DSGVO und eines gerichtlichen Rechtsbehelfs gemäß Art. 79 Abs. 1 DSGVO in derselben Sache unzulässig ist, weshalb die Beschwerde seitens der DSB zurückgewiesen wurde.

Das Bundesverwaltungsgericht hat die Bescheidbeschwerde im Ergebnis abgewiesen, jedoch aus anderen Gründen.

Zur „Doppelgleisigkeit" des Rechtsschutzes wurde auf das Urteil des OGH vom 23. Mai 2019, 6 Ob 91/19d, verwiesen, wonach der OGH die Zulässigkeit dieser Doppelgleisigkeit bereits bejaht habe. Deshalb geht das Bundesverwaltungsgericht davon aus, dass auch bei gleichem Streitgegenstand eine Inanspruchnahme des Beschwerderechts bei der Datenschutzbehörde und eine Klage zulässig seien. Es wird darauf verwiesen, dass „eine Zweigleisigkeit ausdrücklich gewollter Regelungsinhalt der DSGVO ist". Eine Entscheidungskompetenz der Datenschutzbehörde sei daher grundsätzlich zu bejahen.

Dieses Erkenntnis ist nicht rechtskräftig, es wurde seitens der Datenschutzbehörde mit Amtsrevision bekämpft.

W256 2235360-1/5E, Erkenntnis vom 18. Dezember 2020 („AMS-Algorithmus")
Zum Bescheid der Datenschutzbehörde siehe oben (3.2.5. Amtswegige Prüfverfahren)

Das Bundesverwaltungsgericht hat der Beschwerde des AMS Folge gegeben und den Bescheid der Datenschutzbehörde ersatzlos behoben.

Begründend führte das Bundesverwaltungsgericht zusammengefasst aus, dass das AMS nach § 25 Abs. 1 AMSG grundsätzlich berechtigt sei, eine Bewertung von Arbeitsmarktchancen der Arbeitssuchenden anhand (bestimmter) personenbezogener Daten vorzunehmen. Eine unterschiedliche Beurteilung der Rechtmäßigkeit allein wegen der Form ihrer Verarbeitung (automatisiert oder nicht automatisiert) sei im Gesetz grundsätzlich nicht vorgesehen. Der in Art. 22 DSGVO geregelte Fall einer automatisierten Entscheidung sei nicht gegeben, da die Entscheidung lediglich unter Zuhilfenahme des „Arbeitsmarktchancen Assistenz-Systems" (AMAS), letztlich jedoch durch die Berater des AMS erfolge. Dass die Berater das Ergebnis des AMAS im Einzelfall routinemäßig übernehmen könnten, sei für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung an sich nicht von Relevanz. Es liege kein Verstoß gegen den in Art. 5 Abs. 1 lit. a DSGVO normierten Grundsatz der rechtmäßigen Datenverarbeitung vor, weshalb der Bescheid aufzuheben sei.

Dieses Erkenntnis ist nicht rechtskräftig, es wurde seitens der Datenschutzbehörde mit Amtsrevision bekämpft.

3.2.6a Beschwerdeverfahren vor dem Bundesverwaltungsgericht in Verwaltungsstrafsachen

Im Berichtszeitraum wurden 8 Beschwerden gegen Straferkenntnisse der Datenschutzbehörde erhoben.

W258 2227269-1 - Erkenntnis vom 26.11.2020
Das Bundesverwaltungsgericht hat einer Beschwerde der Österreichischen Post AG gegen das Straferkenntnis der Datenschutzbehörde vom 23. Oktober 2019, DSB-D550.148, mit Erkennt-

nis vom 26. November 2020, GZ W211 2208885-1/19E, Folge gegeben, die Strafe behoben und das Verfahren eingestellt.

Begründend führte das Bundesverwaltungsgericht aus, dass es die Datenschutzbehörde unterlassen habe, das tatbestandsmäßige, rechtswidrige und schuldhafte Verhalten der beschuldigten juristischen Person einer oder mehreren konkreten natürlichen Personen vorzuwerfen. Dies könne vom Verwaltungsgericht jedoch nicht saniert werden. Ein Vorabentscheidungsverfahren – wie von der Datenschutzbehörde unter näherer Darlegung der sich stellenden unionsrechtlichen Fragestellungen angeregt – sei nicht notwendig, weil Art. 83 Abs. 8 DSGVO auf das (Verfahrens-)Recht der Mitgliedstaaten verweise und es sohin zu einer unterschiedlichen Ausgestaltung der Verfahrensvorschriften in den Mitgliedstaaten kommen könne. Das Erfordernis, einer natürlichen Person die einer juristischen Person zuzurechnenden Verstöße vorzuwerfen, gründe auf einer Verfahrensvorschrift, nämlich § 44a VStG.

Die Datenschutzbehörde hat gegen dieses Erkenntnis eine außerordentliche Revision erhoben

Das Revisionsverfahren war zum Redaktionsschluss beim Verwaltungsgerichtshof anhängig.

W258 2222689-1/17E – Erkenntnis vom 13. Juli 2020
Mit dem gegenständlichen – mündlich verkündeten – Erkenntnis hat das Bundesverwaltungsgericht der Beschwerde gegen ein Straferkenntnis der Datenschutzbehörde vom 7. Juni 2019, GZ: DSB-D550.105/0002-DSB/2018, Folge gegeben und den angefochtenen Bescheid der DSB behoben und das Verwaltungsstrafverfahren formell eingestellt.

Die Datenschutzbehörde verhängte mit dem Spruch des angefochtenen Straferkenntnisses eine Geldbuße gegen eine Betriebsgesellschaft mehrerer Fastfood Restaurants; letztere war in Form einer Gesellschaft mit beschränkter Haftung & Co KG eingerichtet und als datenschutzrechtlich Verantwortliche Stelle für eine Videoüberwachungsanlage im Küchenbereich eines näher bezeichneten Restaurants zu qualifizieren, die nach den Feststellungen der Datenschutzbehörde auch zum Zweck der Mitarbeiterüberwachung eingesetzt wurde und dadurch gegen das absolut geltende Verbot der Mitarbeiterkontrolle gemäß § 12 Abs. 4 Z 2 Datenschutzgesetz – DSG, in der Fassung BGBl. I Nr. 24/2018, eingesetzt wurde, wobei sich letzterer Umstand insbesondere anhand einer Anzeige durch die Arbeiterkammer ergab.

Der erkennende Senat kam im gegenständlichen Fall – nach Befragung des Geschäftsführers und einer Filialleiterin – demgegenüber zum Beweisergebnis, dass eine Kontrolle von Mitarbeitern im vorliegenden Fall tatsächlich nicht möglich war; dies deshalb nicht, da weder die Filialleiterin, noch der Geschäftsführer selbst eine technische Zugriffsmöglichkeit auf die Videodaten hatte und im Büro der Filialleitung kein Monitor zur Echtzeitbetrachtung der Bilddaten vorhanden war. Letztlich habe ausschließlich ein beauftragter IT-Dienstleister auf die Echtzeitbilder Zugriff nehmen können. Da im Ergebnis sohin die Videoüberwachungsanlage von den für die Mitarbeiterkontrolle zuständigen Filialmitarbeitern tatsächlich nicht genutzt werden konnte, behob der erkennende Senat das angefochtene Straferkenntnis ersatzlos und stellte das Verfahren gemäß § 38 VwGVG iVm § 45 Abs. 1 Z 2 VStG ein.

3.2.7 Verfahren über die Meldung der Verletzung des Schutzes personenbezogener Daten

Im Berichtsjahr wurden der Datenschutzbehörde entsprechend Art. 33 DSGVO 860 nationale Sicherheitsverletzungen („Data Breaches“) gemeldet. Dazu kamen 14 Meldungen betreffend grenzüberschreitende Sicherheitsverletzungen sowie 76 Sicherheitsverletzungen, die an andere Aufsichtsbehörden im Unionsgebiet herangetragen wurden und der Datenschutzbehörde

aufgrund von potentieller Betroffenheit iSd Art. 4 Abs. 22 DSGVO im Rahmen eines Verfahrens gemäß Art. 65 DSGVO zur Kenntnis gebracht wurden. Seitens der Betreiber öffentlicher Kommunikationsdienste wurden 60 Sicherheitsverletzungen nach § 95a TKG 2003 gemeldet.

Dabei war ein nicht unwesentlicher Anteil der gemeldeten Vorfälle auf die außerordentliche Belastung im Zusammenhang mit der Covid-19 Pandemie zurückzuführen. Es kam mitunter vermehrt zu Versendungen von E-Mails bzw. Schreiben an falsche Empfänger. Auch viele Vorkommnisse im Zusammenhang mit Ransomware-Angriffen wurden an die Datenschutzbehörde herangetragen, wobei zumeist eine Verschlüsselung von Daten das Ziel zu sein schien - häufig in Konnex mit Lösegeldforderungen. Weiteren gemeldeten Vorfällen lag wiederum eine durch Öffnung von E-Mail-Anlagen eingespielte Schadsoftware zugrunde, welche in weiterer Folge E-Mails (zum Teil mitsamt dem vorherigen Schriftverkehr mit dem jeweiligen Verantwortlichen) an gespeicherte bzw. zuvor verwendete E-Mail-Adressen weiterleitete.

Hintergrund der Regelung des Art. 33 DSGVO ist, dass eine Verletzung einen Schaden - wie beispielsweise Verlust der Kontrolle über personenbezogene Daten, Diskriminierung oder Identitätsdiebstahl - für natürliche Personen nach sich ziehen kann, sofern keine rechtzeitige und angemessene Reaktion erfolgt. Liegt bei einer Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die betroffenen Personen vor, kann die Datenschutzbehörde daher einen Verantwortlichen entsprechend Art 58 Abs. 2 lit. e DSGVO anweisen, eine nach Art. 34 Abs. 1 DSGVO gebotene Benachrichtigung nachzuholen oder bei Gefahr im Verzug einen Mandatsbeschied iSd § 22 Abs. 4 DSG erlassen.

Eine solche Anweisung an den Verantwortlichen sprach die Datenschutzbehörde etwa mit Beschied vom 13. November 2020, GZ: D084.1954, aus. Verantwortlicher war hier ein Therapiezentrum, welches Kinder betreut. Ein kurzfristig unversperrt aufbewahrter Dienstlaptop eines Mitarbeiters war gestohlen worden und darauf befanden sich auch Gesundheitsdaten. Die Eintrittswahrscheinlichkeit eines Schadens für die Rechte und Freiheiten der betroffenen Person war in diesem Fall zwar als gering eingestuft worden, jedoch reicht für das Vorliegen eines hohen Risikos iSd Art. 34 Abs. 1 DSGVO bereits aus, dass die Schadensschwere als hoch einzuschätzen ist.

Auch in einem weiteren Bescheid vom November 2020, GZ: D084.2214, sprach die Datenschutzbehörde aus, dass betroffene Personen einer Sicherheitsverletzung infolge eines Cyberangriffs beim Auftragsverarbeiter des Verantwortlichen über den Vorfall zu benachrichtigen sind. Hier war es infolge der Cyberattacke zu einem (Teil-)Datenverlust gekommen. Insbesondere hat eine Benachrichtigung dann zu erfolgen, wenn Daten verschlüsselt und in weiterer Folge nicht wiederhergestellt werden können.

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. Sie kann etwa 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 2020 wurde die Datenschutzbehörde als Aufsichtsbehörde in einem Fall gemäß Art. 36 DSGVO konsultiert. Der Verantwortliche plant die Errichtung einer Teststellung, bestehend aus einem Sensor- und Videoaufnahmesystem, welches im Bereich von Eisenbahnbrücken, die über öffentliche Verkehrsflächen verlaufen, angebracht werden soll. Das System diene der Erkennung und Video-Dokumentation von Schadenfällen, die durch den Zusammenprall eines Fahrzeugs mit einer Brücke verursacht würden (Anpralldetektion). Die Bildaufnahmen würden auch öffentliche Verkehrsflächen erfassen. Das Verfahren wurde im Februar 2021 beendet und wird im nächsten Datenschutzbericht ausführlich erörtert.

3.2.9 Anträge auf Genehmigung von Verhaltensregeln

Verhaltensregeln stellen Leitlinien einer guten Datenschutzpraxis dar und können die datenschutzrechtliche Verhaltensweise von Verantwortlichen und Auftragsverarbeitern innerhalb einer spezifischen Branche standardisieren. Ein wesentliches Kriterium von Verhaltensregeln ist die obligatorische Überwachung dieser Verhaltensregeln. Es sind daher Verfahren vorzusehen, die es einer Überwachungsstelle („monitoring body“) ermöglichen, die Bewertung sowie die regelmäßige Überprüfung der Einhaltung von Verhaltensregeln durchzuführen.

Seit Geltung der DSGVO wurden insgesamt zwölf Anträge auf Genehmigung solcher Verhaltensregeln bei der 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.

Im Berichtszeitraum wurden für vier der aufschiebend bedingt genehmigten Verhaltensregeln dazugehörige Überwachungsstellen akkreditiert. Eine Aufzählung findet sich auf der Website der Datenschutzbehörde.[7] Darüber hinaus hat auch der Europäische Datenschutzausschuss ein Register von Verhaltensregeln aller Mitgliedstaaten veröffentlicht, welches laufend ergänzt wird.[8]

Insgesamt wurden auf nationaler Ebene folgende Verhaltensregeln (bedingt oder unbedingt) genehmigt:

- Verhaltensregeln für Internet Service Provider (Überwachungsstelle vorhanden)
- Verhaltensregeln für die Ausübung des Gewerbes der Adressverlage und Direktmarketingunternehmen gem. § 151 Gewerbeordnung 1994 (Überwachungsstelle vorhanden)
- Verhaltensregeln für Garagen- und Parkplatzbetriebe
- Verhaltensregeln für Netzbetreiber bei der Verarbeitung von mit intelligenten Messgeräten erhobenen personenbezogenen Daten von Endverbrauchern nach den §§ 83 ff. ElWOG 2010
- Verhaltensregeln für Presse- und Magazin-Medienunternehmen (teils nicht rechtskräftig)
- Verhaltensregeln für Bilanzbuchhaltungsberufe (Bilanzbuchhalter, Buchhalter, Perso-

7 Verzeichnis gemäß Art. 40 Abs. 6 DSGVO unter https://www.dsb.gv.at/aufgaben-taetigkeiten/genehmigung-von-verhaltensregeln/Verzeichnis-der-genehmigten-Verhaltensregeln.html

8 https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_de

nalverrechner; Überwachungsstelle vorhanden)
- Verhaltensregeln zum Datenschutz der Berufsvereinigung der ArbeitgeberInnen privater Bildungseinrichtungen (Überwachungsstelle vorhanden)

Ausgehend von den bisherigen Anträgen zeichnet sich ab, dass der Frage der datenschutzrechtlichen Rollenverteilung (unter Berücksichtigung datenschutzrechtlicher Materiengesetze), den Modalitäten und der Ausübung von Betroffenenrechten nach Kapitel III DSGVO, der Umsetzung der Informationspflicht 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 personenbezogenen Daten an Drittländer oder an internationale Organisationen nach Art. 46 Abs. 2 lit e DSGVO war bis zum jetzigen Zeitpunkt noch nicht Gegenstand von Verhaltensregeln.

Im Berichtszeitraum wurde die Website der Datenschutzbehörde überarbeitet und ein „Frage und Antworten" Bereich zum Thema „Verhaltensregeln und Überwachungsstellen" erstellt.[9]

In diesem Bereich wird auch auf die praxisrelevante Frage eingegangen, ob es mehrere Überwachungsstellen für dieselben Verhaltensregeln geben kann. Die Datenschutzbehörde geht – in Einklang mit den Leitlinien des EDSA (siehe unten) – davon aus, dass es für dieselben branchenspezifischen Verhaltensregeln dem Grunde nach mehrere Überwachungsstellen geben kann. Dies unter der Voraussetzung, dass sich die Inhaber von Verhaltensregeln nicht gegen die Akkreditierung einer spezifischen Überwachungsstelle aussprechen, oder ausdrücklich ihre Unterstützung für nur einen anderen Akkreditierungswerber bekunden.

Die Entscheidung darüber, ob es für spezifische Verhaltensregeln mehrere Überwachungsstellen geben kann, liegt somit bei den Inhabern von Verhaltensregeln (vgl. dazu mit näherer Begründung den Bescheid der Datenschutzbehörde vom 28. September 2020, GZ: 2020-0.605.768, abrufbar im RIS).

Weiterführende Informationen zu diesem Thema sind auch in den Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679[10] des EDSA zu finden.

3.2.10 Die Verhängung von Geldbußen durch die Österreichische Datenschutzbehörde

Seit dem 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.

Zu den verfolgten Rechtsverletzungen

Unrechtmäßige Bilddatenverarbeitung durch Private

Auch im Jahr 2020 stellten in Verfahren gegen Privatpersonen der (unrechtmäßige) Betrieb von Bildverarbeitungsanlagen, wie etwa Videoüberwachungseinrichtungen in und außerhalb von privaten Gebäuden sowie in Fahrzeugen installierte Kamerasysteme (sog. Dash-Cams), einen

9 https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_de

10 https://www.dsb.gv.at/europa-internationales/europaeischer_datenschutzausschuss_edsa.html

wesentlichen Anteil der geführten Verfahren zur Verhängung von Geldbußen gemäß Art. 83 DSGVO dar.

Dabei zeigt sich weiterhin, dass vielen privaten Verantwortlichen nicht bewusst ist, dass der Einsatz von Videoüberwachungsanlagen, etwa zur Überwachung des Außenbereiches ihres Wohnhauses oder ihrer Wohnung, wenn vom jeweiligen Aufnahmebereich auch Bereiche des umliegenden öffentlichen Raumes, wie Gehsteige und Straßenteile bzw. Teile einer benachbarten privaten Liegenschaft aufgenommen werden, in das Grundrecht auf Datenschutz von Dritten eingreift. Ein solcher Eingriff kann 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.

Erzeugen von Bilddaten mit Smartphone auf öffentlicher Toilette
In einem Fall verhängte die Datenschutzbehörde eine Geldbuße gegen einen männlichen Benutzer einer öffentlichen Damentoilette, der die Kamerafunktion seines Mobiltelefons dazu benutzte, um eine Benutzerin einer Toilettenkabine zu beobachten, indem er sein Mobiltelefon mit geöffneter Kamera-Applikation unter der Kabinentrennwand durchschob, um die dort befindliche weibliche Person auf dem Display des Smartphones sehen zu können. Im konkreten Fall sprach die Datenschutzbehörde aus, dass die unrechtmäßige Verarbeitung von personenbezogenen (Bild-)Daten bereits durch den oben beschriebenen Vorgang verwirklicht wurde, ohne dass (nachweislich) Bilddaten auf dem Speicher des Mobiltelefons zur allfälligen späteren Betrachtung und Weiterverarbeitung dauerhaft gespeichert wurden (vgl. Bescheid vom 14. September 2020, GZ: 2020-0.550.332, RIS).

Zugriff auf Polizeiakten durch Beamte ohne dienstliche Veranlassung
In mehreren Fällen verhängte die Datenschutzbehörde Geldbußen gegen Bedienstete der Polizei, da diese Einsicht in das elektronische Aktensystem der Polizei genommen haben, ohne dass die jeweils Beschuldigten hierfür eine dienstliche Veranlassung – etwa in Form eines von ihnen als zuständigem Sachbearbeiter zu bearbeitenden Aktenvorganges – belegen konnten. Die Beschuldigten und (datenschutzrechtlich Verantwortlichen) haben durch den widerrechtlichen Zugriff und die im weiteren Verlauf erfolgte Einsichtnahme personenbezogene Daten unrechtmäßig sowie zweckwidrig verarbeitet. Die in den jeweiligen Akten enthaltenen personenbezogenen Daten (insbesondere die Namen von Beschuldigten, Geschädigten und an der jeweiligen Amtshandlung beteiligten Beamten) stellen zweifelsfrei personenbezogene Daten im Sinne von Art. 4 Z 1 DSGVO dar. Die in den vorliegenden Fällen erfolgte Einsichtnahme in Aktenvorgänge war als Verarbeitung personenbezogener Daten im Sinne des Art. 4 Z 2 DSGVO zu qualifizieren. Die Beschuldigten waren für diese konkreten Verarbeitungsvorgänge in rechtlicher Hinsicht als Verantwortliche im Sinne von Art. 4 Z 7 DSGVO anzusehen, da durch sie selbst – und nicht durch den Dienstgeber – ein persönliches Informationsinteresse an den abgefragten Daten gegeben war. Im Ergebnis überwogen bei der vorzunehmenden Interessenabwägung im Sinne von Art. 6 Abs. 1 lit. f DSGVO jedenfalls die Schutzinteressen der von dem jeweiligen Verarbeitungsvorgang betroffenen Personen.

Offenlegung von schulbezogenen Daten durch einen Lehrer im Rahmen einer Whats-App Gruppe
Eine Geldbuße richtete sich gegen einen als Lehrer tätigen Beschuldigten, der unrechtmäßig und zweckwidrig personenbezogene Daten verarbeitet hat, indem er eine Videoaufzeichnung angefertigt hatte, in der er personenbezogene Daten minderjähriger Schüler und deren Erziehungsberechtigten einer zukünftigen ersten Klasse, aus einer Liste vorgelesen hat, wobei in der Videoaufzeichnung auch die Liste zu sehen war und diese Videoaufzeichnung in weiterer Folge mittels der Applikation „WhatsApp“ im Rahmen einer dortigen Gruppe verbreitet hatte.

Im Ergebnis wurden dadurch die Grundsätze der Verarbeitung von personenbezogenen Daten auf rechtmäßige Weise, nach Treu und Glauben (Art. 5 Abs. 1 lit. a DSGVO), der Verarbeitung von personenbezogenen Daten für festgelegte, eindeutige und legitime Zwecke (Art. 5 Abs. 1 lit. b DSGVO) sowie der Verarbeitung von personenbezogenen Daten in einer Weise, die dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt ist (Art. 5 Abs. 1 lit. c DSGVO), verletzt.

Dies dadurch, dass die von der Veröffentlichung der personenbezogenen Daten betroffenen Schüler und deren Angehörige naturgemäß nicht in eine derartige Datenverarbeitung eingewilligt haben und auch sonst keiner der von Art 6 Abs. 1 DSGVO abschließend normierten Erlaubnistatbestände gedeckt war.

Offenlegung von E-Mailadressen in großer Anzahl durch offenen E-Mailverteiler
In einer weiteren Entscheidung hatte die DSB die verwaltungsstrafrechtliche Verantwortung eines gemeinnützigen Vereins als beschuldigte juristische Person und datenschutzrechtlich Verantwortlicher zu beurteilen.

Im Rahmen des Versandes einer E-Mailnachricht über die Adresszeile wurde ein gesamter E-Mailverteiler, bestehend aus über 1.400 E-Mailadressen von Vereinsmitgliedern, sämtlichen Empfängern offengelegt, ohne dass die betroffenen Personen in eine derartige Offenlegung eingewilligt haben und ohne dass diese Offenlegung auf einen sonstigen Erlaubnistatbestand des Art. 6 Abs. 1 DSGVO gestützt werden konnte.

Durch die Offenlegung der E-Mailadressen im oben beschriebenen Ausmaß hatte der beschuldigte Verein daher im Ergebnis die Verletzung des in Art 5 Abs. 1 lit. a DSGVO normierten Grundsatzes der „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“ und der abschließend in Art. 6 Abs. 1 DSGVO normierten Erlaubnistatbestände zu verantworten.

Die ausgewiesenen organschaftlichen Vertreter des Vereins haben die Einhaltung der datenschutzrechtlichen Bestimmungen, bezogen auf den Versandvorgang, nicht im geeigneten Ausmaß durch Kontrolle und Überwachung der für den Verein tätigen Personen sichergestellt. Das rechtswidrige und schuldhafte Verhalten der organschaftlichen Vertreter wurde dabei der beschuldigten juristischen Person im Sinne von § 30 Abs. 1 und Abs. 2 DSG zugerechnet.

Von der Verhängung einer Geldbuße wurde im gegenständlichen Fall abgesehen und eine Verwarnung im Sinne von Art. 58 Abs. 2 lit. b DSGVO ausgesprochen. Dies aufgrund der bisherigen verwaltungsstrafrechtlichen Unbescholtenheit des Beschuldigten sowie der Tatsache, dass Maßnahmen zur Vermeidung zukünftiger Verstöße ergriffen wurden, indem der Vorstand seit dem Vorfall derartige Versandvorgänge selbst beaufsichtigt und für die Verwaltung der Mitgliederdaten des Vereins eine geeignete Softwarelösung eingesetzt wird.

Verspätete Meldung einer Sicherheitsverletzung
Eine Geldbuße verhängte die Datenschutzbehörde gegen eine im Bereich der Sozialdienstleistungen tätige GesmbH, da dieser ein Sicherheitsvorfall gemäß Art. 33 DSGVO bereits am 23. Oktober 2019 bekannt war, dieser Vorfall der Datenschutzbehörde jedoch erst Ende April 2020 gemeldet wurde.

Rechtlich folgte daraus, dass die Verantwortliche jedenfalls gegen ihre aus Art. 33 DSGVO resultierende Verpflichtung verstoßen hat, wonach im Falle einer Verletzung des Schutzes personenbezogener Daten der Verantwortliche eine solche Verletzung unverzüglich und möglichst

binnen 72 Stunden, nachdem dem Verantwortlichen die Verletzung bekannt wurde, diese der Datenschutzbehörde als zuständiger Aufsichtsbehörde zu melden hat.

Die verwaltungsstrafrechtliche Verantwortung der beschuldigten GmbH ergab sich daraus, dass die im Firmenbuch ausgewiesenen organschaftlichen Vertreter der Verantwortlichen der aus Art. 33 Abs. 1 DSGVO resultierenden Meldeverpflichtung selbst nicht zeitgerecht nachgekommen sind, und dass mangelnde Kontrolle und Überwachung der im Firmenbuch ausgewiesenen organschaftlichen Vertreter dazu geführt hat, dass auch die zuständigen Mitarbeiterinnen und Mitarbeiter der aus Art 33 Abs. 1 DSGVO resultierenden Meldeverpflichtung nicht zeitgerecht nachgekommen sind.

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.

- Bundesgesetz, mit dem das Gesundheitstelematikgesetz 2012 und das Bundesgesetz BGBl. I Nr. 37/2018 geändert werden
- Bundesgesetz, mit dem das Hochschul-Qualitätssicherungsgesetz geändert wird, ein Bundesgesetz über Privathochschulen erlassen wird und das Fachhochschul-Studiengesetz sowie das Hochschulgesetz 2005 geändert werden
- Vorarlberger Gesetz über Sozialleistungen für hilfsbedürftige Personen - Sammelgesetz
- Änderung des PStSG und Erlassung der Vertrauenswürdigkeitsprüfungs-Verordnung
- Entwurf eines Bundesgesetzes, mit dem ein Investitionskontrollgesetz erlassen und das Außenwirtschaftsgesetz 2011 geändert wird
- Bundesgesetz, mit dem ein neues Tierärztegesetz erlassen und das Tierärztekammergesetz geändert wird
- Bundesgesetz, mit dem das E-Government-Gesetz und das Passgesetz 1992 geändert werden
- Bundesgesetz, mit dem zivilrechtliche und zivilprozessuale Maßnahmen zur Bekämpfung von Hass im Netz getroffen werden (Hass-im-NetzBekämpfungs-Gesetz – HiNBG)
- Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen
- Bundesgesetz, mit dem das Epidemiegesetz 1950, das Tuberkulosegesetz und das COVID-19-Maßnahmengesetz geändert werden
- Entwurf eines Landesgesetzes, mit dem das Gesetz über die Gewährung von Sozialunterstützung (Steiermärkisches Sozialunterstützungsgesetz – StSUG) erlassen und das Steiermärkische Sozialhilfegesetz, das Steiermärkische Wohnunterstützungsgesetz, Steiermärkische Behindertengesetz und das Steiermärkische Grundversorgungsgesetz geändert werden
- Neufassung der Verordnung des Fachverbandes der gewerblichen Dienstleister über die Befähigungsprüfung für das Sicherheitsgewerbe eingeschränkt auf das Gewerbe der Berufsdetektive (Berufsdetektive-Befähigungsprüfungsordnung)
- Bundesgesetz, mit dem das Kontenregister- und Konteneinschaugesetz, das Finanzmarkt-Geldwäschegesetz, das Bankwesengesetz, die Bundesabgabenordnung, das Finanzmarktaufsichtsbehördengesetz und das Wertpapieraufsichtsgesetz 2018 geändert werden
- Bundesgesetz, mit dem ein Investitionskontrollgesetz erlassen und das Außenwirtschaftsgesetz 2011 geändert wird
- Bundesgesetz, mit dem das Hochschul-Qualitätssicherungsgesetz geändert wird, ein Bundesgesetz über Privathochschulen erlassen wird und das Fachhochschul-Studiengesetz sowie das Hochschulgesetz 2005 geändert werden

- Erneuerbaren-Ausbau-Gesetz (EAG-Paket)
- Gesamtreform des Exekutionsrechts
- Bundesgesetz, mit dem ein Bundesgesetz zur Finanzierung der Digitalisierung des österreichischen Schulwesens (DigiSchG) beschlossen wird
- Verordnung des Bundesministers für Finanzen über die Abfrage von sensiblen Daten 2020 nach dem Transparenzdatenbankgesetz 2012 (Transparenzdatenbank-Abfrageverordnung 2020)
- Bundesgesetz, mit dem das Bildungsdokumentationsgesetz 2020 erlassen wird und das Schulpflichtgesetz 1985, das Pflichtschulabschluss-Prüfungs-Gesetz, das Hochschulgesetz 2005, das Hochschul-Qualitätssicherungsgesetz, das Universitätsgesetz 2002, das IQS- Gesetz sowie das Anerkennungs- und Bewertungsgesetz geändert werden
- Bundesgesetz, mit dem ein Bundesgesetz zur Verhinderung von Doping im Sport (AntiDoping-Bundesgesetz 2021 – ADBG 2021) erlassen und das Bundesgesetz betreffend die Förderung des Sports (Bundes-Sportförderungsgesetz 2017 – BSFG 2017) geändert werden

4 Wesentliche höchstgerichtliche Entscheidungen

4.1 Verfahren vor dem Verfassungsgerichtshof

Im Berichtszeitraum sind folgende datenschutzrechtlich relevante Entscheidungen des Verfassungsgerichtshofes ergangen:

4.1.1 Beschluss vom 25.2.2020, G 84/2020 ua

In dieser Sache wurde ein gegen elektrizitätsrechtliche Gesetze und Verordnungen sowie gegen Allgemeine Geschäftsbedingungen von Elektrizitätsunternehmen gerichteter Individualantrag auf Normenprüfung eingebracht. Diesen hat der VfGH mangels Darlegung und Zuordnung der Bedenken sowie mangels eines tauglichen Anfechtungsgegenstandes zurückgewiesen. Der Antragsteller hatte in seinem Antrag u.a. vorgebracht, durch die Pflicht zur Installation eines intelligenten Messgerätes („Smart Meter“) in seinen Rechten gemäß Art. 8 EMRK und § 1 DSG verletzt zu sein.

4.1.2 Beschluss vom 26.11.2020, E 3828/2019

In dieser Sache, deren Ausgangspunkt der Bescheid der Datenschutzbehörde vom 17.7.2017, GZ. DSB-D122.682/0006-DSB/2017, war (Abweisung der Datenschutzbeschwerde, Berichtigung eines Geburtsdatums für leistungsrelevante Zwecke der Sozialversicherung nur auf Grundlage von § 358 ASVG), hat der VfGH die inhaltliche Behandlung der gegen das abweisende Erkenntnis des BVwG vom 4.9.2019, W101 2168337-1, eingebrachten (Erkenntnis-) Beschwerde gemäß Art. 144 Abs. 2 B-VG abgelehnt. Die DSB hatte in diesem Verfahren eine Gegenschrift eingebracht.

4.2 Oberster Gerichtshof

Der OGH hat im Berichtsjahr das erste österreichische Vorabentscheidungsersuchen (Art. 267 AEUV) zur DSGVO gestellt.

4.2.1 Beschluss vom 25.11.2020, 6 Ob 77/20x

Eine zur Klagsführung gemäß § 29 KSchG berechtigte Verbraucherschutzorganisation begehrte gerichtlich, einem Unternehmen (Autovermietung) die Verwendung mehrerer Vertragsklauseln in AGB und Vertragsformularen zu untersagen, weil diese gegen Art. 25 Abs. 2 DSGVO verstoßen würden. Die Gegenpartei bestritt u.a. unter Verweis auf die von Österreich nicht genutzte Öffnungsklausel des Art. 80 Abs. 2 DSGVO die Legitimation zur Klagsführung.

Die Vorinstanzen sahen die Klage als zulässig (und berechtigt) an.

Der OGH hat nunmehr im Revisionsverfahren beschlossen, dem EuGH gemäß Art. 267 AEUV folgende Frage zur Vorabentscheidung vorzulegen:

„Stehen die Regelungen in Kapitel VIII, insbesondere in Art. 80 Abs. 1 und 2 sowie Art. 84 Abs. 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, ABl. L 119/1 vom 4. Mai 2016, S. 1; im Folgenden „DSGVO“) nationalen Regelungen entgegen, die – neben den Eingriffsbefugnissen der zur Überwachung und Durchsetzung der Verordnung zuständigen Aufsichtsbehörden und den Rechtsschutzmöglichkeiten der betroffenen Personen – einerseits Mitbewerbern und andererseits nach dem nationalen Recht berechtigten Verbänden, Einrichtungen und Kammern die Befugnis einräumen, wegen Verstößen gegen die DSGVO unabhängig von der Verletzung konkreter Rechte einzelner betroffener Personen und ohne Auftrag einer betroffenen Person gegen den Verletzer im Wege einer Klage vor den Zivilgerichten unter den Gesichtspunkten des Verbots der Vornahme unlauterer Geschäftspraktiken oder des Verstoßes gegen ein Verbraucherschutzgesetz oder des Verbots der Verwendung unwirksamer Allgemeiner Geschäftsbedingungen vorzugehen?“

4.3 Verwaltungsgerichtshof

Der VwGH hat im Berichtsjahr eine Entscheidung getroffen, die Einfluss auf die Umsetzung und Effektivität der Strafbestimmung des Art. 83 DSGVO in Österreich haben wird.

4.3.1 Beschlüsse vom 27.1.2020, Ro 2018/04/0007, und vom 24.4.2020, Ra 2017/04/0143

In beiden Fällen hat der VwGH Revisionen (der Parteien des Beschwerdeverfahrens vor der DSB) gegen Erkenntnisse des BVwG in Datenschutzsachen mangels Aufzeigung einer Rechtsfrage von grundsätzlicher Bedeutung zurückgewiesen (Art. 133 Abs. 4 B-VG, § 34 Abs. 1 VwGG). Zusammen mit einem weiter unten berichteten Beschluss geht aus dieser Rechtsprechung hervor, dass der VwGH an den Nachweis von Gründen für die Zulässigkeit einer Revision auch in Datenschutzsachen und im Fall der Zulassung der Revision durch das BVwG einen strengen Maßstab anlegt.

4.3.2 Erkenntnis vom 12.5.2020, Ro 2019/04/0229

Dieses Erkenntnis ist aufgrund einer Amtsrevision der DSB (gegen das Erkenntnis des BVwG vom 19.8.2019, W211 220885-1, „Wettcafé-Fall“) ergangen. Das Höchstgericht hat dabei die Revision abgewiesen und die Argumente der DSB großteils verworfen. § 30 DSG sei, anders als von der DSB unter Berufung auf den Anwendungsvorrang des Unionsrechts vorgebacht, im Verfahren zur Verhängung von Geldbußen gemäß Art. 83 DSGVO in vollem Umfang anzuwenden. Die DSB müsse eine oder mehrere bestimmte natürliche Personen ermitteln, verfolgen und deren Schuld nachweisen, um einer juristischen Person deren Verhalten zurechnen und eine Strafe gegen letztere verhängen zu können (das Verfahren gegen die natürlichen Personen sei gleichzeitig gemäß § 30 Abs. 3 DSG einzustellen). Diese Verfahrensschritte könnten nicht im Verfahren vor dem Verwaltungsgericht nachgeholt werden. Das BVwG habe richtigerweise auf die vorliegende Rechtsprechung des VwGH zu § 99d des Bankwesengesetzes (BWG) verwiesen und rechtmäßig auf Aufhebung des Straferkenntnisses der DSB und Einstellung des Verwaltungsstrafverfahrens entschieden.

Diese für die DSB national bindende Auslegung von Art. 83 DSGVO iVm § 30 DSG wurde vorgenommen, ohne eine Vorabentscheidung des EuGH zur Auslegung von Art. 83 DSGVO einzuholen. Rechtsprechung des EuGH liegt hier (noch) nicht vor, und die Auslegung von Art. 83 DSGVO ist unionsweit bisher uneinheitlich, wobei eine Tendenz zu bestehen scheint, die Frage der Strafbarkeit einer juristischen Person anders zu lösen, als das österreichische Höchstgericht (z.B. Frankreich, Conseil d‘État, 19.6.2020, N°430810, Google LLC gg CNIL [Frage der Zurechnung des schuldhaften Verhaltens einer natürlichen Person war kein Thema]; explizit gegensätzlich: Deutschland, Landgericht Bonn, 11.11.2020, 29 OWi 430 Js-OWi 366/20-1/20 LG).

Bis zu einer endgültigen Auslegung von Art. 83 DSGVO durch den EuGH wird die DSB in Verwaltungsstrafverfahren gegen juristische Personen, insbesondere Unternehmensträger, mit deutlich höherem Aufwand ermitteln.

4.3.3 Beschluss vom 5.6.2020, Ro 2018/04/0023

Mit diesem Beschluss hat der VwGH eine vom BVwG ausdrücklich zugelassene (ordentliche) Amtsrevision der DSB zurückgewiesen, da die Revision „letztlich keine für den Verfahrensausgang relevante und somit ihre Zulässigkeit begründende Rechtsfrage“ aufzeige. Dies, weil entgegen der Rechtsansicht der DSB der vom BVwG festgestellte Sachverhalt rechtlich selbst im Lichte des DSG 2000 zu einer Stattgebung der Beschwerde führen hätte müssen (das BVwG hatte auf den Sachverhalt, einen Eingriff in das Recht auf Geheimhaltung im Jahr 2014, rückwirkend die DSGVO angewendet). In seiner Begründung (Erkenntnis, Rn 23) macht der VwGH (durch Zitate aus seiner Rechtsprechung und jener des EuGH) deutlich, dass die DSGVO nicht auf einen Sachverhalt anzuwenden gewesen wäre, der bereits vor ihrem Wirksamwerden abgeschlossen war.

4.4 Europäischer Gerichtshof für Menschenrechte

4.4.1 Urteil vom 30.1.2020, Breyer gegen Deutschland (Appl. 50001/12)

In dieser Sache ist der EGMR (kleine Kammer) zu dem Schluss gekommen, dass eine Pflicht zur Identifizierung aller Kunden und Verarbeitung von deren (Stamm-) Daten durch Telekom-Unternehmen (Verbot anonymer Prepaid-SIM-Karten), wie sie in Deutschland durch Gesetz im Jahr 2004 eingeführt worden ist (§ 111 dt. TKG, vgl. auch § 97 Abs. 1a TKG 2003), keine Verletzung des Grundrechts gemäß Art. 8 EMRK (Recht auf Schutz des Privat- und Familienlebens)

darstellt. Die entsprechenden deutschen Gesetze würden einen zulässigen Zweck verfolgen und seien hinsichtlich des Umfangs der Grundrechtseingriffe verhältnismäßig.

Ein Antrag der Beschwerdeführer auf neuerliche Entscheidung durch die große Kammer des EGMR ist in weiterer Folge abgelehnt worden.

4.4.2 Beschluss vom 12.5.2020, Ringler gegen Österreich (Appl. 2309/10)

Diese Beschwerde, gerichtet gegen die Auskunftspflicht der Telekomanbieter gegenüber Sicherheitsbehörden gemäß § 53 Abs. 3a und 3b SPG, wurde vom EGMR wegen Nichterschöpfung des innerstaatlichen Instanzenzuges inhaltlich nicht zugelassen. Der EGMR bestätigte damit indirekt einen Beschluss des VfGH aus dem Jahr 2009 (Zurückweisung eines Individualantrags auf Gesetzesprüfung). Die Beschwerdeführerin habe es unterlassen, gegen eine behauptete unzulässige Verarbeitung ihrer Daten innerstaatlich mit einer Beschwerde bei der Datenschutzbehörde (bzw. vor 2014 bei der Datenschutzkommission) und in weiterer Folge vor den zuständigen nationalen Gerichten vorzugehen.

4.5 Europäischer Gerichtshof

Der EuGH hat im Berichtsjahr mehrere über den jeweiligen Anlassfall hinausreichende Entscheidungen getroffen. Einerseits hat er ausgesprochen, dass auch Organe der gesetzgebenden Gewalt bei Datenverarbeitungen für Zwecke ihrer verfassungsmäßigen Aufgaben die DSGVO zu befolgen haben, andererseits hat er in Fragen der Anerkennung der Gleichwertigkeit der Datenschutzgesetze von Drittstaaten und der Zulässigkeit staatlicher Überwachungsmaßnahmen neuerlich den Normsetzern verdeutlicht, dass in die Garantien des Datenschutz-Grundrechts der EU (Art. 8 GRC) nur in sehr engen Grenzen eingegriffen werden darf.

Der für die Auslegung der DSGVO in den Mitgliedstaaten des Europäischen Wirtschaftsraums (EWR) zuständige EFTA-Gerichtshof hatte Fragen des Beschwerdeverfahrens gemäß Art. 77 DSGVO (Zulässigkeit der anonymen Beschwerdeführung, Reichweite der garantierten Unentgeltlichkeit der Beschwerdeführung) zu entscheiden.

4.5.1 Urteil vom 9.7.2020, C-272/19 (VQ gegen Land Hessen)

Grundlage dieses Verfahrens war ein Vorabentscheidungsersuchen des Verwaltungsgerichts Wiesbaden (Deutschland). Der dortige Kläger hatte einen Auskunftsantrag gemäß Art. 15 DSGVO an den Petitionsausschuss des Landtags des deutschen Bundeslands Hessen gerichtet. Dieser war durch den Landtagspräsidenten abgelehnt worden, wogegen eine Klage eingebracht wurde. Bedeutsam war die dem EuGH vorgelegte Frage, ob der Petitionsausschuss ein Verantwortlicher gemäß Art. 4 Z 7 DSGVO ist, und ob die DSGVO auf den Sachverhalt überhaupt Anwendung findet.

Der EuGH hat diese Fragen klar bejaht: ein parlamentarischer Ausschuss ist Verantwortlicher, soweit er *„allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet“*, die DSGVO sei daher anzuwenden. Laut EuGH seien weiters die Einschränkungen der sachlichen Anwendbarkeit der DSGVO gemäß Art. 2 Abs. 2 lit a *„eng auszulegen“.*

4.5.2 Urteil vom 16.7.2020, C-311/18 (Schrems II)

Ausgangspunkt des Verfahrens war ein Rechtsstreit zwischen der irischen Aufsichtsbehörde (DPC) und Maximilian Schrems im Hinblick auf die von Herrn Schrems begehrte Untersagung

der Übermittlung seiner personenbezogenen Daten durch Facebook Irland an Facebook Inc. in die Vereinigten Staaten. Der EuGH prüfte aus diesem Anlass auf Grundlage eines Vorabentscheidungsersuchens des High Court (irisches Rechtsmittelgericht für Streitigkeiten mit der DPC) einerseits die Gültigkeit der Angemessenheitsentscheidung der Europäischen Kommission betreffend die USA (Beschluss 2016/1250, sog. „Privacy Shield") und andererseits den Beschluss 2010/87 über Standarddatenschutzklauseln für Auftragsverarbeiter (sog. „SDK-Beschluss").

Im Ergebnis wurde der Beschluss betreffend das „Privacy Shield" (wie bereits jener zu dessen Vorgänger „Safe Harbor") für ungültig erklärt. Als maßgeblich für seine Entscheidung nennt der Gerichtshof umfangreiche, nicht auf das zwingend erforderliche Maß beschränkte Eingriffs- und Zugriffsbefugnisse von U.S.-amerikanischen Behörden auf personenbezogene Daten, welche aus dem Unionsgebiet in die Vereinigten Staaten übermittelt werden, sowie unzureichende Rechtsschutzmöglichkeiten.

Im Hinblick auf den SDK-Beschluss hielt der EuGH fest, dass die Prüfung anhand der Charta der Grundrechte nichts ergeben hat, was seine Gültigkeit berühren könnte. Gleichzeitig sprach der Gerichtshof aber aus, dass Standarddatenschutzklauseln alleine in bestimmten Fällen kein ausreichendes Schutzniveau bieten und daher die Schaffung von zusätzlichen Maßnahmen bzw. Garantien geboten sein kann.

Der Europäische Datenschutzausschuss hat zum Urteil C-311/18 bereits am 23. Juli 2020 ein Dokument mit häufig gestellten Fragen veröffentlicht.

4.5.3 Urteil vom 6.10.2020, C-511/18 ua (La Quadrature du Net) und C-623/17 (Privacy International)

Dem ersten Urteil lagen Vorabentscheidungsersuchen des Conseil d'État (Staatsrat, oberstes französisches Verwaltungsgericht) und der Cour Constitutionelle (belgischer Verfassungsgerichtshof) zu Grunde. Bei diesen Gerichten waren mehrere Rechtstreitigkeiten von Organisationen und Einzelpersonen mit Staatsorganen in Frankreich und Belgien anhängig. In der zweiten Sache war ein Vorabentscheidungsersuchen des Investigatory Powers Tribunal (britisches Aufsichtsgericht für Nachrichtendienste und Überwachungsmaßnahmen) in einem Streit zwischen einer privaten Datenschutzorganisation und britischen Staatsorganen Anlass des EuGH-Verfahrens.

Hauptfrage war jeweils die Auslegung von Art. 15 der Richtlinie 2002/587EG (Datenschutzrichtlinie für elektronische Kommunikation, E-Privacy-Richtlinie), der Einschränkungen von Datenschutzrechten für Zwecke der nationalen Sicherheit, der Landesverteidigung, der öffentlichen Sicherheit sowie der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen vorsieht, unter anderem auch die (fakultative) Einführung einer Pflicht zur Vorratsdatenspeicherung.

Der EuGH kam in seinen Entscheidungen, aufbauend auf eigener Vorjudikatur, zu dem Schluss, dass eine anlasslose Vorratsdatenspeicherung mit den grundlegenden Menschenrechten auf Privatsphäre, Datenschutz und Meinungsfreiheit nicht vereinbar und daher unzulässig ist. Davon dürfe die nationale Gesetzgebung nur in sehr engen Grenzen (bei ernsthafter, vorhersehbarer Bedrohung der nationalen Sicherheit, zur Bekämpfung schwerer Straftaten, zur Abwehr schwerwiegender Bedrohungen der öffentlichen Sicherheit) Ausnahmen vorsehen, die auch IP-Adressen umfassen und auf das absolut erforderliche Zeitmaß beschränkt bleiben müssten. Bei konkretem Terrorverdacht sei auch die Auswertung von Echtzeit-Daten einer Person nach vorheriger Prüfung durch ein Gericht oder eine unabhängige Behörde zulässig.

4.5.4 Urteil vom 11.11.2020, C-61/19 (Orange Romania)

Ausgangsverfahren war die Klage eines Mobilfunkunternehmens gegen eine von der rumänischen Aufsichtsbehörde für Datenschutz (ANSPDCP) verhängte Geldbuße, die Vorlage erfolgte durch das rumänische Rechtsmittelgericht.

Strittig war die Frage der Rechtmäßigkeit der Einwilligung der betroffenen Person in die Aufbewahrung von Ausweiskopien (Papierkopien).

Der EuGH knüpft in der Beantwortung der Vorlagefragen hier an seine Entscheidung in der Sache „Planet49" (Urteil vom 1.10.2019, C-673/17) an. Den Verantwortlichen treffe die Beweislast für die gesetzmäßige Information der betroffenen Person und die Freiwilligkeit von deren Einwilligung (Art. 5 Abs. 2, Art. 7 Abs. 1 DSGVO). Bei einer Einwilligung müsse es sich um eine aktive und unmissverständliche Willenshandlung handeln. Ein Vertragsformular dürfe nicht über die Möglichkeit, den Vertrag auch ohne eine Einwilligung in eine Datenverarbeitung abzuschließen, irreführen. Die freie Entscheidung des Betroffenen dürfe nicht durch das Verlangen von Zusatzerklärungen bei verweigerter Einwilligung beeinträchtigt werden.

4.5.5 EFTA-Gerichtshof, Urteil vom 10.12.2020, E-11/19 und E-12/19 (Adpublisher AG)

Ausgangsverfahren waren zwei Streitverfahren vor der liechtensteinischen Beschwerdekommission für Verwaltungsangelegenheiten (kurz: Beschwerdekommission, zuständiges Verwaltungsgericht). Die im Bereich Onlinemarketing tätige Adpublisher AG hatte darin Entscheidungen der Datenschutzstelle von Liechtenstein (federführende Aufsichtsbehörde gemäß Art. 56 DSGVO) hinsichtlich von Beschwerden der in Deutschland niedergelassenen betroffenen Personen J und K (wegen der behaupteten Verletzung der Art. 5, 6 und 15 DSGVO) angefochten. Die betroffenen Personen waren im Verfahren vor der Datenschutzstelle und der Beschwerdekommission gegenüber der Adpublisher AG nicht namentlich genannt worden.

Der Beschwerdekommission legte die Frage, ob aus der DSGVO zu entnehmen ist, dass eine solche anonyme Beschwerdeführung überhaupt zulässig ist, sowie die Folgefrage, ob besondere Gründe für die Anonymisierung prima facie festgestellt werden müssen, dem EFTA-Gerichtshof zur Vorabentscheidung vor.

Der EFTA-Gerichtshof entschied diesbezüglich, dass die DSGVO der Offenlegung der personenbezogenen Daten eines Beschwerdeführers im Zuge eines Verfahrens aufgrund einer Beschwerde nach Artikel 77 der DSGVO oder eines Verfahrens nach Artikel 78 Absatz 1 der DSGVO nicht entgegensteht. Die Frage der Zulässigkeit einer anonymen Beschwerdeführung sei mit Blick auf die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 und 6 DSGVO zu prüfen. Eine anonyme Beschwerdeführung dürfe jedenfalls nicht bewilligt werden, wenn dadurch die Erfüllung der Verpflichtungen gemäß der DSGVO behindert oder Grundsätze eines ordnungsgemäßen, rechtsstaatlichen Verfahrens verletzt würden.

Eine weitere Vorlagefrage betraf die Frage, ob sich die Garantie der Unentgeltlichkeit des Beschwerdeverfahrens für die betroffene Person (Art. 57 Abs. 3 DSGVO) auch auf eine verfahrensrechtlich zulässige Kostenentscheidung im Rechtsmittelverfahren erstreckt.

Der EFTA-Gerichtshof hat hierzu ausgesprochen, dass einer betroffenen Person keinerlei Kosten auferlegt werden dürfen, wenn ein Verantwortlicher einen Rechtsbehelf gegen eine Entscheidung der Aufsichtsbehörde eingelegt hat.

5 Datenschutz-Grundverordnung und Datenschutzgesetz – Erfahrungen und legistische Maßnahmen

5.1 Erfahrungen der DSB im Berichtszeitraum

Auf die Auswirkungen der Covid-19-Pandemie auf die Tätigkeit der DSB wird gesondert eingegangen.

Dieser Abschnitt widmet sich den allgemeinen Erfahrungen und wesentlichen Ereignissen im Berichtszeitraum.

5.1.1 DSB verbleibt beim Bundesministerium für Justiz

Die Regierungsbildung des Kabinetts „Kurz II“ Anfang 2020 hatte insoweit Auswirkungen auf die DSB, als die Zuständigkeit für allgemeine Angelegenheiten des Schutzes personenbezogener Daten beim Bundesministerium für Justiz (BMJ) verblieb und die DSB nach wie vor diesem Ressort zugeordnet ist. Dies hat jedoch lediglich Implikationen dahingehend, dass die Bundesministerin für Justiz die politische Verantwortung für Tätigkeiten der DSB gegenüber dem Nationalrat trägt; ein (inhaltliches) Weisungsrecht ist damit nicht verbunden, weil es sich bei der DSB um eine weisungsfreie Verwaltungsbehörde nach Art. 51 ff DSGVO handelt.

5.1.2 Verfahrenszahlen und Personalstand

Nach dem massiven Anstieg der Verfahrenszahlen in den Jahren 2018 und 2019 gingen sie im Berichtsjahr 2020 leicht zurück und pendelten sich auf hohem Niveau ein.

Gleichzeitig ist es dem beharrlichen Einsatz der Bundesministerin für Justiz zu verdanken, dass die DSB im Jahr 2020 insgesamt 12 zusätzliche Planstellen erhalten hat (10 für den höheren Dienst, 2 für den gehobenen Dienst); zusätzlich wurden wie bereits in den Jahren 2018 und 2019 Budgetmittel für 5 Verwaltungspraktikanten bereitgestellt. Die zusätzlichen Planstellen konnten im Jahr 2020 teilweise bereits besetzt werden. Mit dem Abschluss der Besetzungsverfahren ist mit März 2021 zu rechnen.

Das Jahr 2020 brachte somit eine merkbare Erleichterung der bis dato sehr angespannten personellen Situation, die auch von der Volksanwaltschaft anerkannt und als Missstand in der Verwaltung bewertet worden ist.

Ein Gutteil der anhängigen Verfahren betrifft nach wie vor Beschwerdeverfahren gegen die Österreichische Post AG im Zusammenhang mit der 2019 bekannt gewordenen Verarbeitung personenbezogener Daten betreffend die statistische Errechnung der vermeintlichen politischen Affinität.

Darüber hinaus war das Jahr 2020 geprägt von einer Entscheidung des Verwaltungsgerichtshofes zur unmittelbaren Strafbarkeit einer juristischen Person nach Art. 83 DSGVO; auf diese Entscheidung wird an anderer Stelle ausführlich eingegangen werden. Die Rechtsansicht des

Verwaltungsgerichtshofes hat zur Folge, dass Verwaltungsstrafverfahren gegen juristische Personen eines erhöhten verfahrensrechtlichen Aufwandes bedürfen.

Abgesehen davon war das Berichtsjahr von einer Verdoppelung der Verfahren vor dem BVwG sowie einem deutlichen Anstieg der Entscheidungen des BVwG geprägt, die teilweise (Amts) Revisionsverfahren vor dem VwGH nach sich zogen.

Ebenso konnte ein Anstieg an Vorabentscheidungsverfahren vor dem EuGH verzeichnet werden, zu welchen die DSB vom innerstaatlich federführenden Ressort, dem Bundeskanzleramt-Verfassungsdienst, regelmäßig um fachliche Stellungnahme ersucht wurde.

5.1.3 Tätigkeiten für den Europäischen Datenschutzausschuss

Pandemiebedingt fanden die Sitzungen und Besprechungen des EDSA ab März 2020 ausschließlich im Rahmen von Videokonferenzen statt, wobei dies der inhaltlichen Tätigkeit des Ausschusses und seiner Untergruppen keinen Abbruch tat.

Im Gegenteil: In der Hochphase des ersten europaweiten Lockdowns im März 2020 fanden Plenarsitzungen, die im Regelfall einmal monatlich abgehalten werden, im Wochenrhythmus statt. Insgesamt wurden im Jahr 2020 mehr als 25 Sitzungen des EDSA und mehr als 100 Sitzungen seiner Untergruppen auf ExpertInnenebene abgehalten.

Ein Blick auf die Website des EDSA belegt darüber hinaus, dass im Jahr 2020 wesentliche Stellungnahmen erarbeitet und verabschiedet wurden. Die DSB ist in allen Untergruppen des Ausschusses vertreten, die Leiterin ist seit Mai 2018 Vorsitzende des Europäischen Datenschutzausschusses.

5.1.4. Erster Bericht der Kommission zur Bewertung und Überprüfung der DSGVO

Ebenfalls im Jahr 2020 wurde der erste Bericht der Europäischen Kommission nach Art. 97 DSGVO zur Bewertung und Überprüfung der DSGVO, COM(2020) 264 final[11] vorgelegt. Einbezogen wurden dabei auch die Stellungnahme des EDSA[12] sowie die Stellungnahmen einzelner Aufsichtsbehörden, darunter jene der DSB.[13]

Die DSGVO wurde jedoch keiner gesamten Bewertung unterzogen, sondern es wurden schwerpunktmäßig die Anwendung und die Funktionsweise der Vorschriften über die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen (Kapitel V DSGVO) sowie die Vorschriften über die Zusammenarbeit und Kohärenz (Kapitel VII) analysiert. Zusammenfassend bewertet die Kommission die DSGVO als wesentlichen Meilenstein zur Gewährleistung des Schutzes personenbezogener Daten, ortet aber teilweise noch eine zu starke Fragmentierung in den Rechtsordnungen der Mitgliedstaaten sowie Potential, die Zusammenarbeit zwischen den Aufsichtsbehörden stärker auszubauen. Gleichzeitig hält sie aber fest, dass es für eine allfällige Novelle der DSGVO zu früh ist und weitere Erfahrungen abzuwarten sind.

5.1.5. Urteil des EuGH zu „Schrems 2“

Ein weiteres wesentliches Ereignis stellte das am 16. Juli 2020 erlassene Urteil des EuGH in Rechtssache C-311/18 („Schrems 2“) dar, mit welchem die die USA betreffende Adäquanzentscheidung für internationale Datenübermittlungen („Privacy Shield“) für ungültig erklärt wur-

11 Abrufbar in Deutsch unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0264&from=EN

12 Abrufbar in Englisch unter https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

13 Siehe https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

de. Sowohl die DSB als auch der EDSA haben darauf umgehend reagiert und stellen einschlägige Informationen für den Datenaustausch mit den USA bereit.[14]

5.1.6. Grenzüberschreitende Zusammenarbeit und erster verbindlicher Beschluss des EDSA

Bei grenzüberschreitenden Verfahren gelangt das strukturierte Verfahren nach Art. 56 ff iVm Art. 60 DSGVO zur Anwendung. Seit Beginn des In Geltung Tretens der DSGVO im Mai 2018 betraf dies insgesamt 512 anhängig gemachte Verfahren von denen bis Ende 2020 168 mit „final decisions" beendet werden konnten.

Im dritten Jahr der Anwendung der DSGVO haben sich diese Verfahren bei den Aufsichtsbehörden „eingespielt", auch wenn es punktuell Verbesserungsbedarf gibt. Die DSGVO regelt zwar die Pflicht der Aufsichtsbehörden zur Zusammenarbeit, legt aber – von wenigen Ausnahmen abgesehen – keine verfahrensrechtlichen Vorschriften dazu fest. Da jede Aufsichtsbehörde ihr nationales Verfahrensrecht zur Anwendung bringt (sofern es solche gibt), führt dies zu Konstellationen, in denen die Pflicht zur Zusammenarbeit an ihre Grenzen stößt: So ist bspw. die DSB verpflichtet, alle relevanten Beweismittel (v.a. Eingaben der Gegenparteien) einem Beschwerdeführer im Rahmend es Parteiengehörs zur Kenntnis zu bringen, damit sich dieser dazu äußern kann. In anderen Verfahrensordnungen ist diese Pflicht nicht vorgesehen, sodass der DSB fallweise erst auf mehrmaliges Urgieren hin von federführenden Aufsichtsbehörden relevante Dokumente übermittelt werden, damit die DSB ihrerseits diese einem Beschwerdeführer zugänglich machen kann.

2020 wurde erstmals ein Verfahren nach Art. 65 DSGVO, basierend auf maßgeblichen und begründeten Einsprüchen (darunter auch einen der DSB) gegen den Beschlussentwurf der irischen Aufsichtsbehörde, ausgelöst. Der Ausschuss fasste am 9. November 2020 den Beschluss 1/2020, mit welchem einige Einsprüche als begründet anerkannt wurden.[15]

5.1.7. Schengen-Evaluierung 2020

Die ursprünglich für das Frühjahr 2020 angesetzte, alle fünf Jahre stattfindende Evaluierung durch eine gemischte Kommission (zusammengesetzt aus Vertretern der Europäischen Kommission, des Europäischen Datenschutzbeauftragten sowie von anderen Aufsichtsbehörden) musste pandemiebedingt in den Herbst verschoben werden. Aufgrund der anhaltend angespannten epidemiologischen Lage fand die Evaluierung ausschließlich auf elektronischem Weg in der Woche vom 16.-20. November 2020 statt. Dabei wurde die DSB an einem der Evaluierungstage einer intensiven Prüfung dahingehend unterzogen, ob sie die Einhaltung der Regeln der SIS II-Verordnung[16] wirksam überprüft und Betroffenenanfragen nachkommt. Der Bericht über die Evaluierung ist bei Redaktionsschluss noch ausständig.

5.2 Zertifizierungsstellen-Akkreditierungs-Verordnung

Im Berichtszeitraum wurde der Entwurf einer Verordnung der Datenschutzbehörde über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle (Zertifizierungsstellen-Akkreditierungs-Verordnung

14 Siehe https://www.dsb.gv.at/aufgaben-taetigkeiten/internationaler-datenverkehr.html mit weiteren Hinweisen

15 Abrufbar in Englisch unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_bindingdecision01_2020_en.pdf

16 Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)

– ZeStAkk-V) zur allgemeinen Begutachtung versendet und dem EDSA zur Stellungnahme nach Art. 64 DSGVO vorgelegt.

Die ZeStAkk-V wurde nach Abschluss dieses Prozesses im BGBl. II Nr. XXX/2021 kundgemacht. Sie regelt, in Durchführung der Vorgaben des Art. 43 Abs. 3 DSGVO und § 21 Abs. 3 DSG, die näheren Details hinsichtlich der Akkreditierung einer Zertifizierungsstelle. Die DSGVO regelt in Art. 43 Abs. 2 in Grundzügen die Anforderungen an eine Zertifizierungsstelle, überlässt aber den nationalen Aufsichtsbehörden die nähere Konkretisierung dieser Vorgaben. Damit diese Vorgaben unionsweit möglichst einheitlich erlassen werden, war der EDSA im Vorfeld zu befassen.

Eine durch die Datenschutzbehörde akkreditierte Zertifizierungsstelle ist befugt, auf Basis der gemäß Art. 42 Abs. 5 DSGVO genehmigten Zertifizierungskriterien Verantwortliche oder Auftragsverarbeiter auf deren Antrag zu zertifizieren.

Der Verordnungstext sowie die Erläuterungen dazu sind auf der Website der DSB abrufbar.[17]

Die Stellungnahme des EDSA (Stellungnahme Nr. 30/2020) ist in englischer Sprache auf der Website des EDSA abrufbar.[18]

5.3 COVID-19 – Erfahrungen, Maßnahmen und Entscheidungen der DSB

5.3.1. Auswirkungen auf die DSB

COVID-19 traf die DSB – so wie faktisch alle Menschen und Behörden – überraschend und in unterschiedlicher Weise.

Anlässlich des ersten Lockdowns Mitte März 2020 hat die Leitung die Entscheidung getroffen, sämtliche Bedienstete der DSB ausschließlich Telearbeit (Homeoffice) verrichten zu lassen. Da die juristischen Bediensteten zu diesem Zeitpunkt bereits durchgehend mit mobilen Endgeräten und Diensthandys ausgestattet waren und für die übrigen Bediensteten diese Geräte mit Unterstützung des BMJ kurzfristig beschafft werden konnten, war ein weitgehend reibungsloser Umstieg vom Präsenz- in den Onlinebetrieb möglich.

Für fünf Wochen verrichteten alle Bediensteten ihren Dienst ausschließlich von zuhause aus. Einmal pro Woche wurde die Post behoben und zur Bearbeitung weitergeleitet.

Die Verfahrensführung mittels Elektronischem Akt (ELAK) durch die DSB hat die Umstellung maßgeblich erleichtert, weil auf diese Weise eine ununterbrochene Aktenbearbeitung möglich war. Allerdings stößt dieses System dort an seine Grenzen, wo nach wie vor auf Papierverarbeitung gesetzt werden muss: Dies betrifft vor allem die Abfertigung jener Schriftstücke, die nicht elektronisch versendet werden können, wie bspw. RSa- und RSb-Briefe. Hier bildete sich ein erheblicher Rückstand, der erst nach der schrittweisen Wiederaufnahme des Präsenzbetriebs in Teams ab Mitte April 2020 versendet werden konnte.

Die Dienstverrichtung von zuhause aus hat deutliche Optimierungspotentiale offenbart: War es bisher üblich, dass die meisten Akten der DSB „dual" – dh. elektronisch und in Papierform – geführt wurden, ist dies nunmehr nur mehr in Ausnahmefällen üblich. Es hat sich gezeigt, dass

17 https://www.dsb.gv.at/recht-entscheidungen/verordnungen-in-oesterreich.html
18 https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-302020-draft-decision-competent_de

eine Verfahrensführung auch ohne umfangreiche Papierakten möglich ist, weshalb Ausdrucke nur mehr dann vorgenommen werden, wenn es sich um umfangreiche Dokumente handelt, die zumutbarerweise nicht ausschließlich im elektronischen Format von Bediensteten gelesen werden können.

Ebenso hat die DSB die elektronische Zustellung gemäß Zustellgesetz – dh. über einen Zustelldienst –forciert: Immer wenn dies möglich ist (bei Rechtsanwälten ist dies durchgehend der Fall), werden Dokumente seitens der DSB ausschließlich auf diesem Weg versendet. Die Vorteile gegenüber der – zulässigen – Übermittlung per E-Mail bestehen darin, dass Dokumente nachweislich übermittelt werden können und in der erhöhten Datensicherheit dieser Übermittlungsmaßnahme.

Von Mitte April bis Mitte Juni 2020 wurde der Dienst in zwei bzw. drei unterschiedlichen, sich alle zwei Wochen abwechselnden Gruppen verrichtet. Im Sommer war ein weitgehend „normaler" Dienstbetrieb möglich. Die steigenden Infektionszahlen im Herbst führten dazu, dass ab Mitte September 2020 wieder auf einen „Schichtbetrieb" mit drei Gruppen umgestellt wurde, wobei dieser Schichtbetrieb zum Zeitpunkt der Verfassung dieses Datenschutzberichts nach wie vor aufrecht ist.

Das wechselnde Arbeiten vor Ort und Teleworking von zu Hause bringt – neben etlichen Vorteilen, wie der möglichen Büronutzung als Einzelzimmer trotz steigender MitarbeiterInnenanzahl – auch deutliche Nachteile: So ist die Koordinierung einzelner Arbeitsgruppen sowie das Abhalten von Besprechungen erheblich erschwert, weil nie gewährleistet ist, dass alle involvierten Personen zeitgleich anwesend sind (aus technischen oder verbindungstechnischen Gründen). Die DSB setzt zwar verstärkt auf Videokonferenzen, jedoch können diese Systeme – trotz vieler Vorteile – persönliche Besprechungen nicht ersetzten.

5.3.2. Rechtliche Fragestellungen und Entscheidungen der DSB

Bereits im März 2020 wurde deutlich, dass COVID-19 nicht nur medizinische, sondern auch rechtliche und vor allem datenschutzrechtliche Fragestellungen aufwirft: Zu klären ist bspw. ob und unter welchen Voraussetzungen Informationspflichten über eine Erkrankung gegenüber dem Dienstgeber bestehen, ob ein Dienstgeber andere Dienstnehmer über einen Infektionsfall informieren darf ja vielleicht sogar muss, was bei Homeoffice zu beachten ist etc.

Die DSB stellt deshalb seit Mitte März 2020 Informationen auf ihrer Website[19] bereit, die regelmäßig aktualisiert werden.

Daneben hat die DSB an einschlägigen Stellungnahmen und Mitteilungen des ESDA mitgewirkt, wobei die Leitlinien 3/2020 über die Verarbeitung von Gesundheitsdaten für Zwecke der wissenschaftlichen Forschung im Kontext von COVID-19[20] , welche die DSB federführend mitgestaltet hat, sowie die Leitlinien 4/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19[21] besonders hervorzuheben sind.

19 https://www.dsb.gv.at/download-links/informationen-zum-coronavirus-covid-19-.html
20 Abrufbar in Englisch unter https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-032020-processing-data-concerning-health-purpose_en
21 Abrufbar in Deutsch unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_de_0.pdf

Im Kontext von COVID-19 war auch die Frage zu klären, ob jene Daten, die im Ergänzungsregister für sonstige Betroffene (ERsB) enthalten sind, zulässigerweise veröffentlicht werden durften. Diese Frage wurde erstmals bei der Beantragung von Wirtschaftshilfen aus dem Härtefall-Fonds virulent und löste eine politische Debatte aus, die ihr vorläufiges Ende darin fand, dass das ERsB nicht mehr als öffentliches Register geführt wird. Einige Betroffene brachten Beschwerden bei der Datenschutzbehörde ein, über die noch nicht entschieden wurde.

Ebenfalls im Zusammenhang mit COVID-19 steht die Frage der so genannten Kontaktnachverfolgung (Contact Tracing), vor allem im Gastronomiebereich. In einigen Bundesländern wurden Gastronomen verpflichtet oder ermächtigt, bestimmte Daten ihrer Gäste zu erheben und sie auf Anfrage den Gesundheitsbehörden zur Verfügung zu stellen, um im Fall einer Infektion mögliche Kontaktpersonen rasch nachverfolgen zu können. Eine betroffene Person brachte deswegen Beschwerde bei der Datenschutzbehörde ein. Dieser Beschwerde wurde stattgegeben[22], weil die entsprechende Verordnung nach Ansicht der Datenschutzbehörde zum damaligen Zeitpunkt keine Deckung im Epidemiegesetz fand.

Zwischenzeitig wurde das Epidemiegesetz – nach Befassung der Datenschutzbehörde – dahingehend novelliert, dass es für die Kontaktnachverfolgung nunmehr eine eindeutige Rechtsgrundlage gibt.[23]

Neben diesen einschlägigen Entscheidungen bzw. Maßnahmen waren und sind zusätzlich jene Vorgaben zu beachten, die für alle Verwaltungsbehörden gelten. Diese finden sich vorwiegend im Verwaltungsrechtlichen COVID-19-Begleitgesetz (COVID-19 VwBG) undlegen unter anderem fest, unter welchen Voraussetzungen mündliche Verhandlungen stattfinden können bzw., dass diese durch Videoschaltungen ersetzt werden können. Daneben finden sich im COVID-19 VwBG Regelungen zur Fristenhemmung bzw. –unterbrechung; damit wurde dem Umstand Rechnung getragen, dass viele Personen in der Zeit von Mitte März bis Ende April 2020 gehindert waren, Verfahrenshandlungen (zeitgerecht) vorzunehmen.

5.3.3. Zusammenfassung

Zusammenfassend war das Jahr 2020 für die DSB in jeglicher Hinsicht von COVID-19 geprägt und wie sicher für alle Menschen und Behörden eine große Herausforderung. Es ist davon auszugehen, dass dies auch auf das Jahr 2021 zutreffen wird, wenngleich wir hoffen, dass auch aufgrund der Möglichkeit der Impfung Entspannung in der Gesamtsituation eintreten wird.

Trotz der unbestrittenen Einschränkungen hat COVID-19 auch dazu geführt, etablierte behördeninterne Prozesse zu überdenken so wurde etwa die innerbehördliche Digitalisierung (weiter) forciert.

Daneben stellten sich von Anbeginn datenschutzrechtliche Fragen, die die DSB zu lösen hatte.

COVID-19 hat auch deutlich gemacht, dass die DSGVO kein Hindernis bei der Bekämpfung einer Pandemie darstellt: Gerade Art. 9, der die Verarbeitung von Gesundheitsdaten regelt, bietet in Abs.2 weitreichende und großzügige Ausnahmen vom grundsätzlichen Verbot der Datenverarbeitung.

22 Siehe die rechtliche Begründung unter https://www.dsb.gv.at/recht-entscheidungen/entscheidungen-der-datenschutzbehoerde.html

23 Siehe § 5c EpiG idF ab BGBl. I Nr. 136/2020

Die DSGVO bildet jedoch auch den zulässigen Rahmen, innerhalb dessen sich Verantwortliche und Auftragsverarbeiter bewegen dürfen. Man kann daher sagen, dass die DSGVO ihre erste diesbezügliche Feuerprobe bestanden hat.

6 Europäische Zusammenarbeit

6.1 Europäische Union

6.1.1 Der Europäische Datenschutzausschuss[24]

Der Der Europäische Datenschutzausschuss (EDSA) hat sich im Jahr 2020, bedingt durch die COVID-19-Pandemie und die damit einhergehenden datenschutzrechtlichen Problemstellungen, statt wie geplant elf Mal, 27 Mal getroffen. Hierbei fanden jedoch nur zwei Treffen vor Ort in Brüssel statt, die restlichen 25 Plenarsitzungen wurden via Videokonferenz abgehalten.

Im Zuge dessen hat der EDSA gemäß Art. 64 Abs. 1 DSGVO 2020 zu folgenden Themen insgesamt 31 Stellungnahmen[25] abgegeben:

- 11 Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Überwachung von Verhaltensregeln gemäß Art. 41 DSGVO (Spanien, Belgien, Frankreich, Deutschland, Irland, Finnland, Italien, Niederlande, Dänemark, Griechenland, Polen);
- 10 Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Zertifizierung gemäß Art. 43 Abs. 3 DSGVO (Vereinigtes Königreich, Luxemburg, Irland, Deutschland, Tschechien, Niederlande, Griechenland, Italien, Dänemark, Österreich);
- eine Stellungnahme zum Entwurf der Standardvertragsklauseln gemäß Art. 28 Abs. 8 DSGVO (Slowenien)
- 9 Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (FAE Group, 2 mal zur Reinsurance Group of America, Jotun, Tetra Pak, Iberdrola Group, Equinix, Coloplast Group, Novelis Group)

Weiters hat der EDSA gemäß Art. 64 Abs. 2 DSGVO[26] 2020 eine Stellungnahme[27] zu nationalen Listen (Frankreich) über Verarbeitungstätigkeiten, die keiner Datenschutz-Folgenabschätzung unterliegen, angenommen.

Zudem hat der EDSA 2020 zu folgenden Themen Leitlinien[28] angenommen:

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

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

26 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

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

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

- Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen (EDPB Guidelines 01/2020)
- Übermittlungen personenbezogener Daten zwischen Behörden und Einrichtungen des EWR und außerhalb des EWR gemäß Art. 46 Abs. 2 lit. a und Abs. 3 lit. b DSGVO (EDPB Guidelines 02/2020)
- Verarbeitung von Gesundheitsdaten zum Zweck der wissenschaftlichen Forschung im Zusammenhang mit dem COVID-19-Ausbruch (EDPB Guidelines 03/2020)
- Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 (EDPB Guidelines 04/2020)
- Einwilligung gemäß Verordnung 2016/679 (EDPB Guidelines 05/2020)
- Zusammenspiel der zweiten Zahlungsdiensterichtlinie und der DSGVO (EDPB Guidelines 06/2020)
- Konzepte des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters in der DSGVO (EDPB Guidelines 07/2020)
- Targeting von Social-Media-Nutzern (EDPB Guidelines 08/2020)
- Erheblicher und begründeter Einwand gemäß Verordnung 2016/679 (EDPB Guidelines 09/2020)
- Beschränkungen gemäß Art. 23 DSGVO (EDPB Guidelines 10/2020)

Darüber hinaus wurden auch zwei Empfehlungen[29] des EDSA zu folgenden Themen angenommen:

- Maßnahmen, zur Ergänzung von Übermittlungsinstrumenten, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten (EDPB Recommendations 01/2020)
- Europäische Grundlegende Garantien für Überwachungsmaßnahmen (EDPB Recommendations 02/2020)

Auch im Jahr 2020 wurden alle Expertenuntergruppen des EDSA seitens der DSB beschickt, jede Expertenuntergruppe traf sich dabei etwa monatlich zur Besprechung, Erarbeitung der Texte und 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 unterliegt gemäß der Europol Verordnung 794/2016[30] einer geteilten Kontrolle: Während die nationalen Kontrollbehörden, die Zulässigkeit der Eingabe und des Abrufs personenbezogener Daten sowie jedweder Übermittlung dieser Daten an Europol überwachen, obliegt dem Europäischen Datenschutzbeauftragten (EDSB), die Überwachung der Verarbeitung durch Europol selbst. 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 Eu-ropol sowie die Verarbeitung dieser Daten durch den betreffenden Mitgliedstaat zu prüfen. Die Vertreter der nationalen Kontrollbehör-

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

30 https://eur-lex.europa.eu/legal-content/dE/ALL/?uri=CELEX:32016R0794

den der Mitgliedstaaten und der Europäische Daten-schutzbeauftragte 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 Perso¬nen bzw. gestohlenen oder verlorenen Sachen, insbesondere Dokumente und Fahrzeuge, im Schen¬gen-Raum auszuschreiben bzw. abzufragen. Die Rechtsgrundlage für das SIS II bildet die sogenannte SIS-II-Verordnung[31]. 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 Bundesminis¬terium 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, wobei sie mindestens alle vier Jahre die Datenverarbeitungsvorgänge auf nationaler Ebene nach internationalen Prüfungsstandards zu überprüfen haben. Darüber hinaus überprüft die Europäische Kommission gemeinsam mit nationalen Experten die Umsetzung der SIS-II-Verordnung in den einzelnen Mitgliedsaaten. Im November 2020 ist die Datenschutzbehörde hinsichtlich der praktischen Umsetzung der relevanten Bestimmungen der SIS-II-Verordnung in ihrem Bereich überprüft worden. Der Abschlussbericht der Europäischen Kommission wird im Jahr 2021 fertiggestellt 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 ne¬ben dem Ausschuss gemäß Art. 43 der ZIS-Verordnung[32] („Joint Supervisory Authority of Customs“ („JSA“)) eine Koordinierende Aufsichtsbehörde (CIS Supervision Coordination Group („CIS-SCG“)) eingerichtet, welche aus Vertretern der nationalen Datenschutzbehörden der Mitgliedstaten 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 Asyl¬werber illegal in die EU eingereist ist. Eurodac besteht aus einer von der Europäischen Kom¬mission verwalteten Zentraleinheit und den in den Mitgliedsstaaten zur Abfrage und Befüllung betriebenen nationalen Systemen. Art. 32 der (EU) Verordnung Nr. 603/2013[33] sieht eine koordinierte Überwachung durch die nationalen Datenschutzbehörden mit dem Europäischen Daten¬schutzbeauftragten vor, wobei die Mitgliedstaaten jährlich eine Überprüfung der Verarbeitung personenbezogener Daten durchzuführen haben.

---

31 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32006R1986
32 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex:31997R0515
33 https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX%3A32013R0603

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[34] (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 Da¬tenschutzbehörden haben gemäß der VIS-Verordnung die Rechtmäßigkeit der Verarbeitung personenbezogener VIS-Daten auf nationaler Ebene zu überwachen, wobei sie mindestens alle vier Jahre die Datenverarbeitungsvorgänge auf nationaler Ebene nach internationalen Prüfungsstandards zu überprüfen haben. Die Datenschutzbehörde hat eine entsprechende Überprüfung Ende 2019 begonnen, aber aufgrund der COVID-19 Pandemie bis dato nicht abschließen können. Die Überprüfung wird in der ersten Jahreshälfte 2021 abgeschlossen werden. Darüber hinaus überprüft die Europäische Kommission gemeinsam mit nationalen Experten die Umsetzung der VIS-Verordnung in den einzelnen Mitgliedstaaten. Im November 2020 ist die Datenschutzbehörde hinsichtlich der Umsetzung der VIS-Verordnung in ihrem Bereich überprüft worden. Der Abschlussbericht wird im Jahr 2021 fertiggestellt werden.

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 fand coronabedingt nur eine Plenarsitzung statt. Diese 40. Plenarsitzung wurde vom 18. bis 20. November 2020 via Videokonferenz abgehalten. Die Tagesordnung sowie der zusammenfassende Bericht der Sitzung 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

Der Europäische Gerichtshof hat mit Urteil vom 16. Juli 2020, C-311/18[35], den Angemessenheitsbeschluss der Europäischen Kommission betreffend die USA („EU-U.S. Privacy Shield“) für ungültig erklärt. Aus diesem Grund erfolgte 2020, anders als in den Vorjahren, keine gemeinsame Überprüfung der Angemessenheitsentscheidung durch die Europäische Kommission und die Vertreter nationaler Aufsichtsbehörden.

Der EDSA nahm die Entscheidung des Europäischen Gerichtshofes jedoch zum Anlass, um Empfehlungen für die, vom Europäischen Gerichtshof in seiner Entscheidung vorgesehenen, „zusätzliche Sicherheitsgarantien“ im Zusammenhang mit internationalen Übermittlungsinstrumenten nach Art. 46 DSGVO zu erarbeiten.[36]

34 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32008R0767
35 Nähere Information zu dieser Entscheidung finden sich im Kapitel 4.4.
36 Diese Empfehlung des EDSA ist unter folgendem Link abrufbar: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en