



Republik Österreich

Datenschutz
behörde

Datenschutzbericht 2021



Datenschutzbericht 2021

Wien, im März 2022

Impressum

Medieninhaber, Herausgeber und Redaktion:

Datenschutzbehörde, Dr. Andrea Jelinek

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

Kontakt: dsb@dsb.gv.at

Website: www.dsb.gv.at

Fotonachweis: Stefanie Korherr (Seite 6)

Gestaltung: Datenschutzbehörde

Druck: BMVRDJ

Wien, 2022

Inhalt

1 Vorwort	5
2 Die Datenschutzbehörde	6
2.1 Organisation und Aufgaben	6
2.1.1 Die Datenschutzbehörde	6
2.1.2 Aufgaben und Befugnisse	6
2.2 Der Personalstand	7
3 Tätigkeit der Datenschutzbehörde	8
3.1 Statistische Darstellung	8
3.2 Verfahren und Auskünfte	13
3.2.1.1 Individualbeschwerden Inland	13
3.2.1.2 Grenzüberschreitende Fälle der DSB	32
3.2.2 Rechtsauskünfte an Bürgerinnen und Bürger	33
3.2.3 Genehmigungen im Internationalen Datenverkehr	34
3.2.4 Genehmigungen nach §§ 7 u. 8 DSG	35
3.2.5 Amtswegige Prüfverfahren	36
3.2.6 Beschwerdeverfahren vor dem Bundesverwaltungsgericht einschließlich Säumnisbeschwerden	38
3.2.6a Beschwerdeverfahren vor dem Bundesverwaltungsgericht in Verwaltungsstrafsachen	42
3.2.7 Verfahren über die Meldung der Verletzung des Schutzes personenbezogener Daten	45
3.2.8 Konsultationsverfahren	46
3.2.9 Anträge auf Genehmigung von Verhaltensregeln	48
3.2.10 Verhängung von Geldbußen durch die Österreichische Datenschutzbehörde: Erfahrungs- und Vollzugsbericht 2021	49
3.2.11 Stellungnahmen zu Gesetzes- und Verordnungsentwürfen	53

4 Wesentliche höchstgerichtliche Entscheidungen	55
4.1 Verfahren vor dem Verfassungsgerichtshof	55
4.2 Oberster Gerichtshof	56
4.3 Verwaltungsgerichtshof	59
4.4 Europäischer Gerichtshof für Menschenrechte	64
4.5 Europäischer Gerichtshof	64
5 Datenschutz-Grundverordnung und Datenschutzgesetz – Erfahrungen und legislative Maßnahmen	68
5.1 Allgemeine Erfahrungen der DSB im Berichtszeitraum, einschließlich Parlamentarischer Anfragen	68
5.1.1 Verfahrenszahlen und Personalstand	68
5.1.2. Vorabentscheidungsersuchen an den EuGH	69
5.1.3. Beschwerden an die Volksanwaltschaft	70
5.1.4. Parlamentarische Anfragen	70
5.1.5. Beschwerden betreffend die so genannte „Islamlandkarte“	70
5.2 COVID-19 – Erfahrungen, Maßnahmen und Entscheidungen der DSB	70
5.2.1. Allgemeine Informationen	70
5.2.2. Rechtliche Fragestellungen und Entscheidungen der DSB	71
6 Europäische Zusammenarbeit	72
6.1 Europäische Union	72
6.1.1 Der Europäische Datenschutzausschuss	72
6.1.2 Europol	79
6.1.3 Schengen	80
6.1.4 Zoll	80
6.1.5 Eurodac	81
6.1.6 Visa	81
6.2 Europarat	81
7 Internationale Beziehungen	82

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 2021 – wie von allen Menschen – nunmehr bereits das zweite Jahr 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.

Die von der Behörde seit März 2020 erarbeiteten FAQs datenschutzrechtlicher Natur die Pandemie betreffend wurden auch im Jahr 2021 permanent überarbeitet und ergänzt und finden sich auf der Website der Behörde. Ich möchte mich an dieser Stelle neuerlich bei all meinen Mitarbeiterinnen und Mitarbeitern für die großartige Zusammenarbeit und die gute Arbeitsdisziplin im Berichtszeitraum bedanken. Ohne ihre kreativen Ideen, technischen Kenntnisse, Fleiß und Engagement wäre es nicht möglich gewesen, die Arbeit in diesem schwierigen Jahr 2021 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. Durch eine im Sommer 2021 durchgeführte konzentrierte Aktion (DSB 2.0.), konnte eine Vielzahl von Verfahren abgeschlossen werden. Siehe hierzu auch die genauen Ausführungen unter 5.2. des Berichts.

Darüber hinaus haben die Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörde im Jahr 2021 sowohl national als auch international unzählige – in den meisten Fällen im Videomodus - Vorträge gehalten und (virtuelle) Veranstaltungen und Konferenzen im Bereich des Datenschutzes besucht.

Das gemeinsam mit der Universität Wien durchgeführte Projekt hat im Jahr 2021 Fahrt aufgenommen und die ersten Zwischenergebnisse wurden bereits intern präsentiert.

Der Datenschutzbericht 2021 ist der achte, 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.

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 Aufgabenbereiche 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 2021 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.

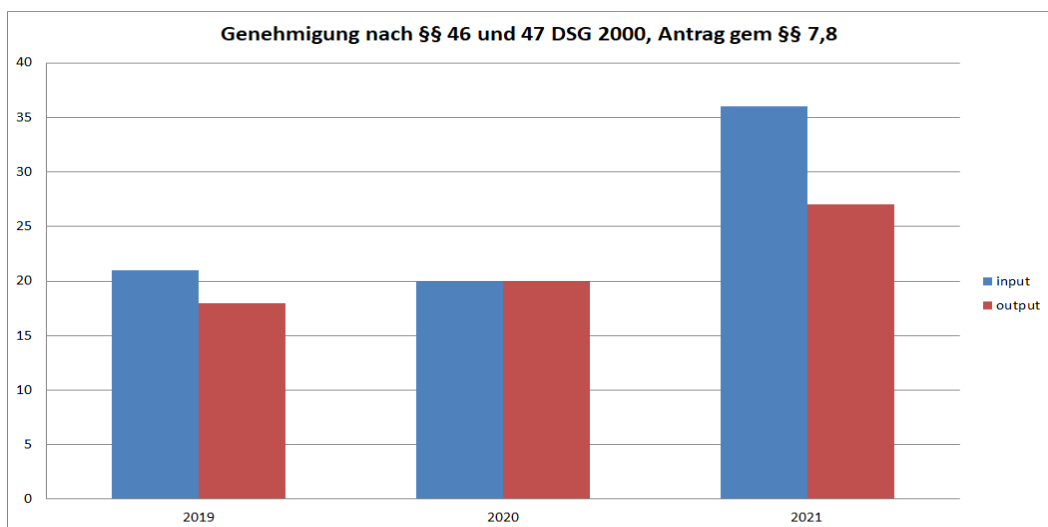
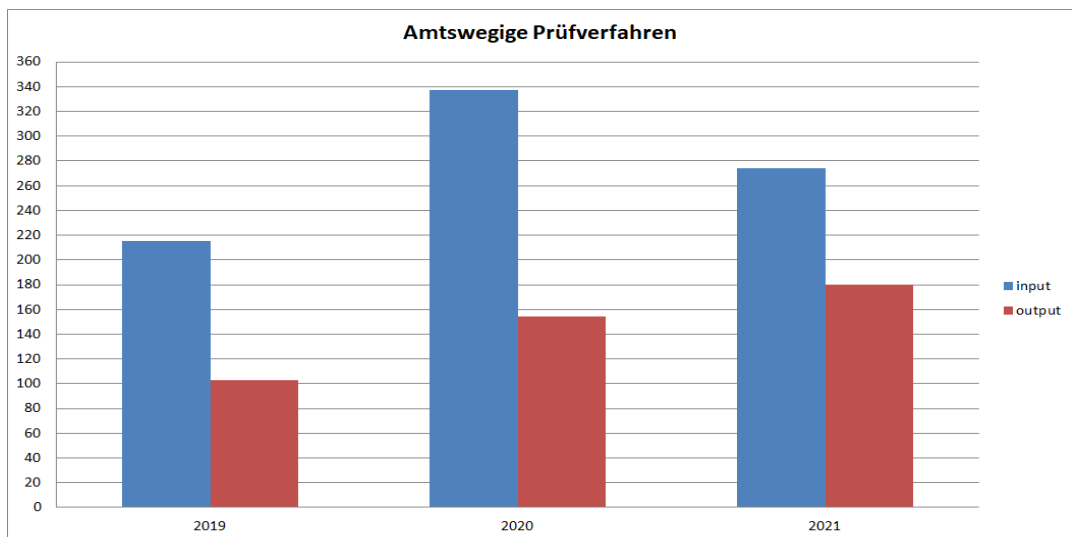
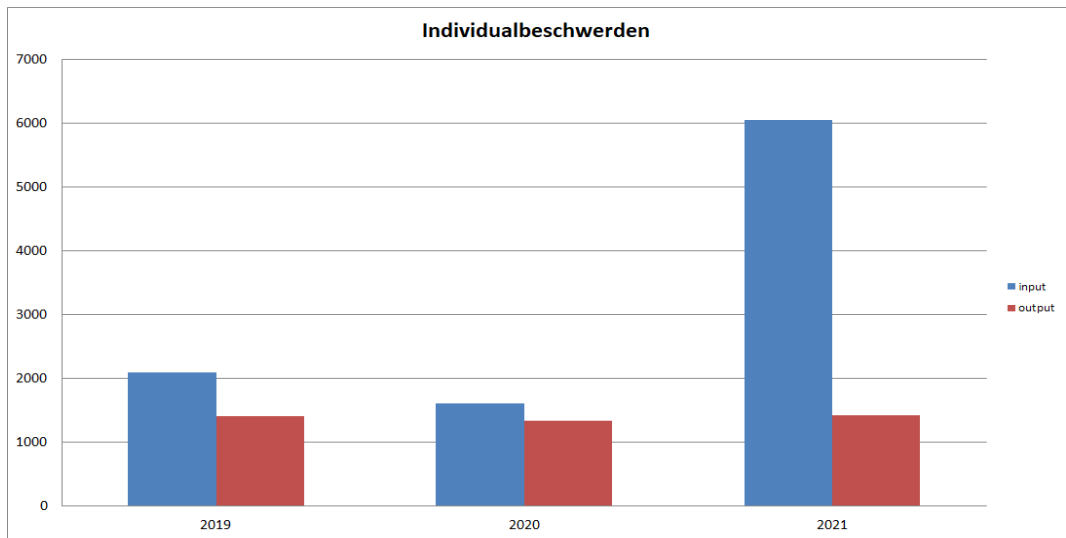
3 Tätigkeit der Datenschutzbehörde

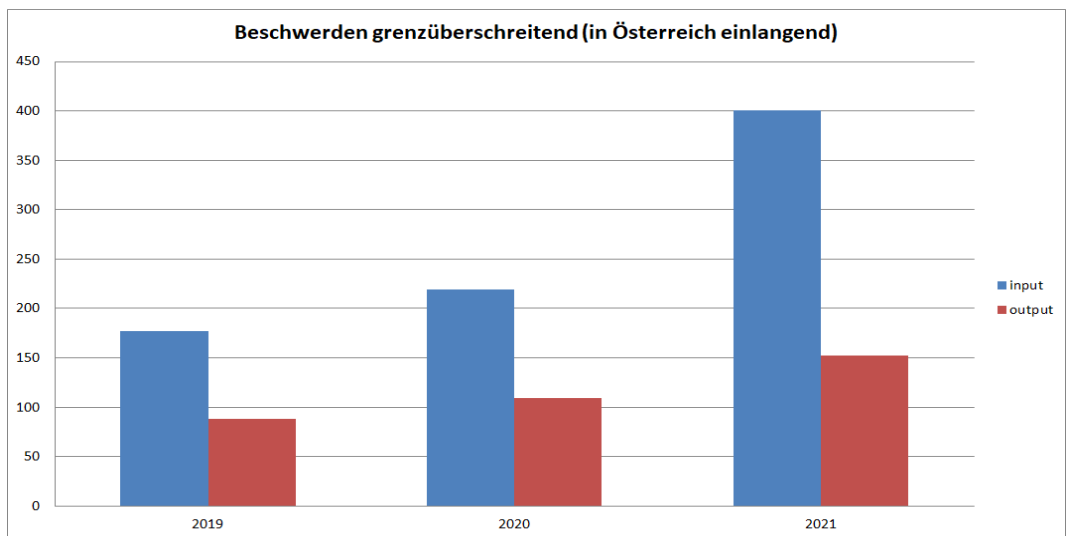
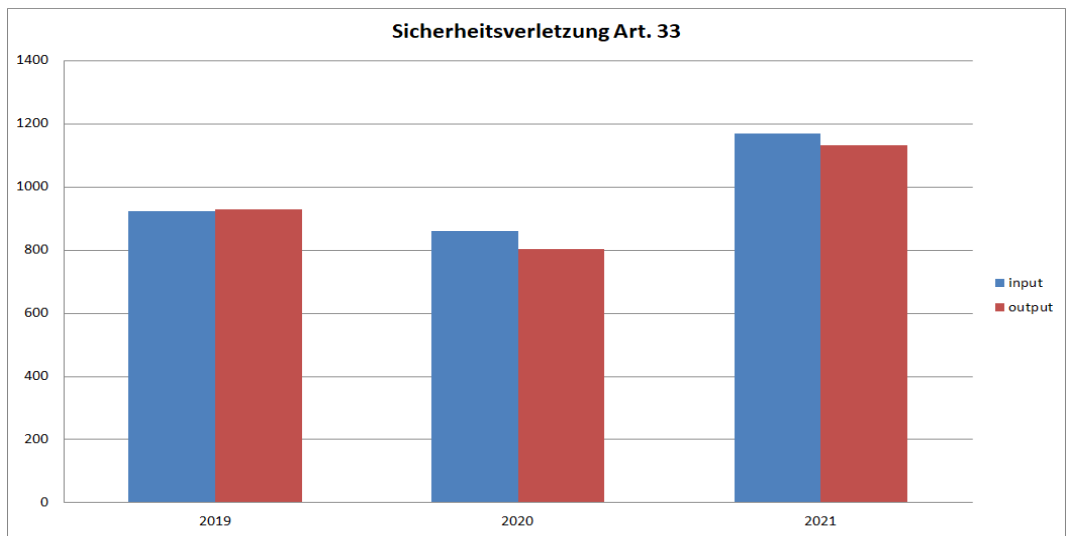
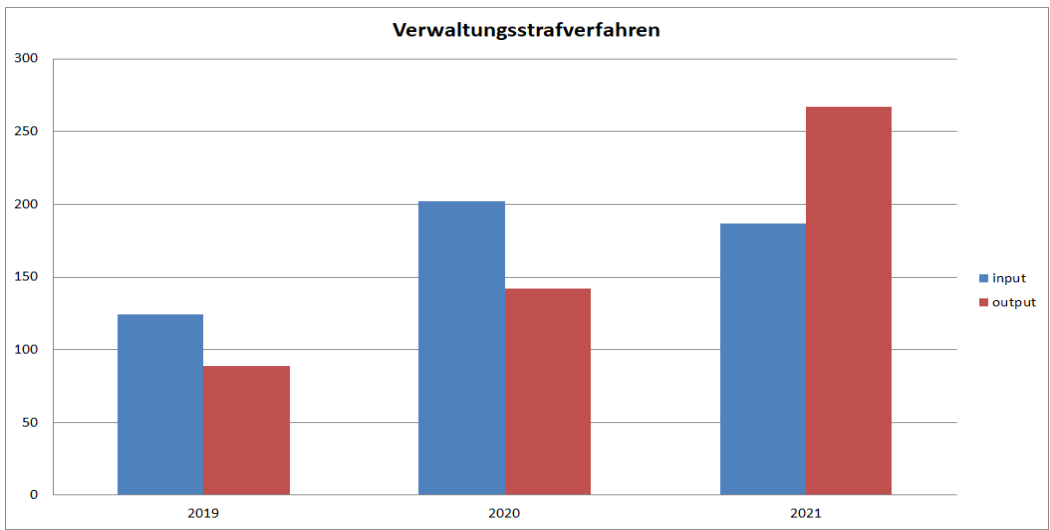
3.1 Statistische Darstellung

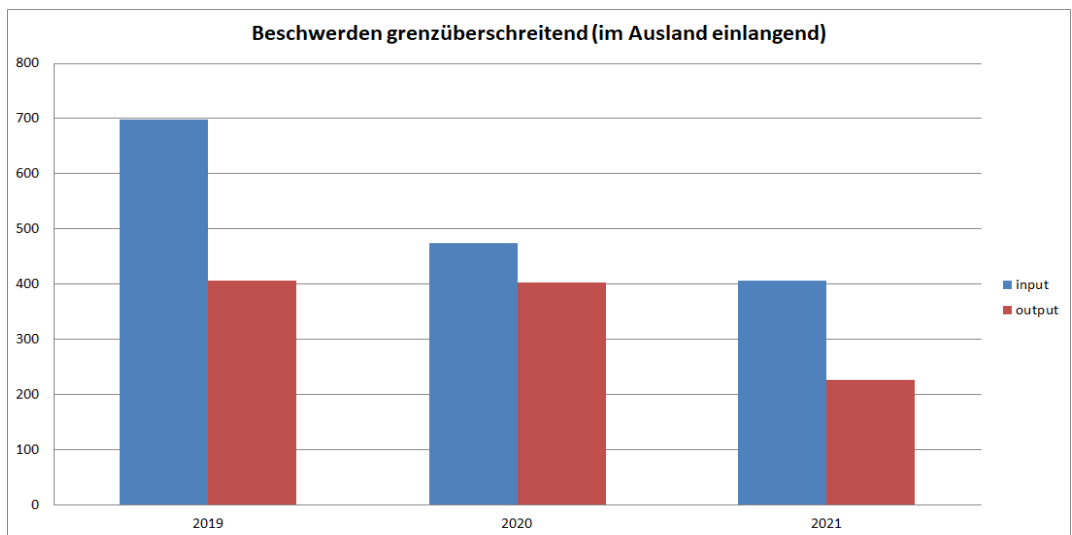
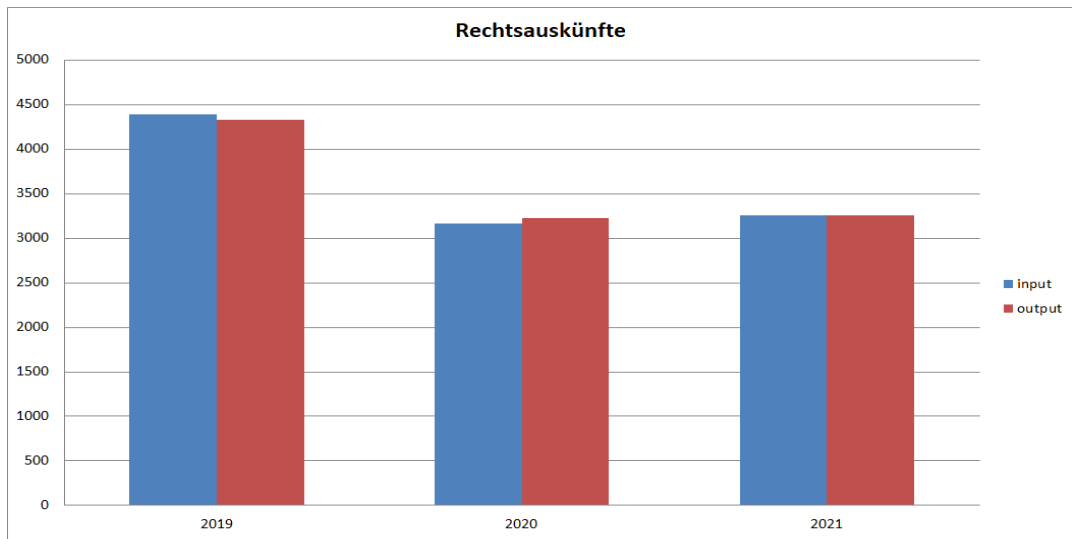
Tabelle 1 Anzahl der Eingangsstücke und Erledigungen

Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2019	2020	2021	2019	2020	2021
Individualbeschwerden	2102	1603	6051	1405	1332	1421
Erledigungsart der Individualbeschwerden				828 Bescheide 577 Einstellungen	852 Bescheide 480 Einstellungen	1036 Bescheide 385 Einstellungen
Beschwerden Grenzüberschreitend (im Ausland einlangend)	698	474	407	407	403	226
Beschwerden Grenzüberschreitend (in Österreich einlangend)	177	219	401	88	109	152
Amtswegige Prüfverfahren	215	337	274	103	154	180
Erledigungsart der Amtswegigen Prüfverfahren						10 Bescheide 170 Einstellungen
Genehmigungen nach §§ 7 und 8 DSG (wissenschaftliche Forschung u. Statistik)	21	20	36	18	20	27
Genehmigungen im Internationalen Datenverkehr	1	0	0	1	0	0
Auskunft Schengen	114	127	117	104	127	117
Verwaltungsstrafverfahren	124	202	190	89	142	267
Erledigungsart der Verwaltungsstrafverfahren (Straferkenntnisse, Strafverfügungen, Verwarnungen, diverse Bescheide wie Wiedereinsetzung, Parteiengehör etc.)						56 Bescheide 211 Einstellungen

Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2019	2020	2021	2019	2020	2021
Standardvertragsklauseln	2	0	0	1	1	0
Verfahren vor dem Bundesverwaltungsgericht	164	319	511			
Sicherheitsverletzungen § 95a	44	60	55	44	61	50
Sicherheitsverletzungen Art 33	923	860	1169	929	802	1131
Sicherheitsverletzungen grenzüberschreitend (in Österreich eingelangend)	11	14	30	14	10	18
Sicherheitsverletzungen grenzüberschreitend (im Ausland einlangend)	71	76	62	41	45	45
Rechtsauskünfte	4384	3166	3257	4329	3227	3257
Allgemeine Anfrage Ausland	40	59	32	33	47	34
Amtshilfeersuchen Ausland			228			137
Anträge auf Genehmigung von Verhaltensregeln	6	2	4	8	2	3
Genehmigung BCR (International)	20	5	0	20	2	0
Konsultationsverfahren	5	1	1	3	1	1
Datenschutzbeauftragte	922	632	626	922	632	626
Verkehr mit Behörden	163	140	137	163	140	137







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

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

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

- die Gesetzgebung von Bund und Ländern (samt zugeordneten Prüfororganen wie Rechnungshof und Volksanwaltschaft)¹
- die Gerichtsbarkeit, soweit sie justizielle Aufgaben (einschließlich Angelegenheiten der Justizverwaltung, die durch Richterkollegien entschieden werden, Art. 87 Abs. 2 B-VG) wahrnimmt,²
- Datenverarbeitungen, die durch natürliche Personen ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten vorgenommen werden³ und
- Datenverarbeitungen für Zwecke der Medienberichterstattung.⁴

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 3.2.10).

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

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

1 Hinweis: Zur Klärung der Frage, ob die DSB als Aufsichtsbehörde für den Nationalrat bzw. dessen Untersuchungsausschüsse in Betracht kommt ist derzeit aufgrund eines Ersuchens des VwGH ein Vorabentscheidungsverfahren beim EuGH zu C-33/22 anhängig.

2 Hinweis: Beim EuGH ist derzeit das Verfahren zu C-245/20 anhängig (Schlussanträge liegen vor), wo es um die Frage der Tragweite der Wortfolge „die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen“ nach Art. 55 Abs. 3 DSGVO geht.

3 Siehe dazu den Bescheid vom 03.05.2021, GZ 2021-0.285.169 (RIS).

4 Siehe dazu den Bescheid vom 21.04.2020, GZ 2020-0.239.741 (RIS).

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 2021

Im Berichtsjahr 2021 wurden insgesamt 6.051 Individualbeschwerden (davon 4.271 Beschwerden ausschließlich im Kontext der Versendung von Schreiben iZm mit der Impfung gegen COVID-19; siehe dazu ausführlich Kapitel 5.1.) bei der Datenschutzbehörde eingebracht. Im Vergleich zum Vorjahr (1.603 Beschwerden) bedeutet dies einen **Anstieg um 277 %**. 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. Die Datenschutzbehörde geht davon aus, dass eine Beschwerdeführung dann als „exzessiv“ zu werten ist, wenn vom selben Beschwerdeführer in einem Durchrechnungszeitraum von 12 Monaten mehr als zwei Beschwerden pro Monat eingebracht werden, somit mehr als 24 Beschwerden pro Jahr.

Ausgewählte Beschwerdeentscheidungen aus 2021

Die DSB hat in ihrer öffentlich zugänglichen Entscheidungsdokumentation (im Rahmen des Rechtsinformationssystems des Bundes – RIS;) aus dem Jahr 2021 5 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 2021 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 10.12.2021, GZ: 2021-0.835.273 (Verfahrenszahl DSB-D124.5337) Juristische Person im selben Umfang wie natürliche Personen gemäß § 1 DSGVO zur Beschwerdeerhebung aktivlegitimiert

Mit diesem Bescheid ist (nicht rechtskräftig) die Beschwerde einer natürlichen und einer juristischen Person (Ges.m.b.H.) gegen zwei Medienunternehmen (Rechtsformen: Ges.m.b.H. bzw. Stiftung öffentlichen Rechts) zurückgewiesen worden. Die Beschwerdeführer hatten Verletzungen in den Rechten auf Geheimhaltung, Auskunft und Löschung geltend gemacht. Es bestand ein enger Bezug zur journalistischen Berichterstattung in den von den Beschwerdegegnerinnen publizierten Medien. Beide Beschwerdegegnerinnen bildeten eine „Recherchegemeinschaft“. Beauskunftet und gelöscht werden sollten Daten im Zusammenhang mit einem Nachweis für eine Datenschutzverletzung bzw. von Verstößen gegen gebotene Datensicherheitsmaßnahmen (Versendung von Gesundheitsdaten per E-Mail), der den Beschwerdegegnerinnen zugespielt und über den berichtet worden war. Auf die Auskunfts- und Löschungsanträge der Beschwerdeführer war seitens der Beschwerdegegnerinnen gar nicht bzw. (unter Hinweis auf das „Medienprivileg“ des § 9 DSGVO) ablehnend reagiert worden.

Die Beschwerdeführer hatten u.a. vorgebracht, dass § 9 DSGVO wegen Verstoß der nationalen Bestimmung gegen Unionsrecht unangewendet zu bleiben habe. Dies wurde von der DSB unter Verweis auf ihre Bindung an geltendes Recht und die ihr fehlende, dem VfGH bzw. EuGH zukommende entsprechende Vorlage- und Prüfkompetenz abgelehnt.

Zum Beschwerderecht einer juristischen Person hat die DSB festgehalten, dass diese zwar grundsätzlich aktiv legitimiert ist, eine Beschwerde nach § 24 DSGVO vor der Datenschutzbehörde zu erheben, sofern sie eine Verletzung der durch § 1 DSGVO gewährleisteten Rechte behauptet, jedoch nur in jenem Umfang, in welchem dies auch einer natürlichen Person möglich wäre. Dies schließt eine Nicht-Anwendung des Medienprivilegs auf solche Beschwerden aus, auch wenn dies vom Wortlaut des § 4 DSGVO gedeckt erscheine.

In der Sache lag eine Beschwerde gegen zwei Medienunternehmen im Zusammenhang mit journalistischer Berichterstattung vor. Letztere umfasst auch den Zweck, einschlägige Dokumente (Rechercheergebnisse) zu archivieren. Daher lag dieser Sachverhalt außerhalb der Zuständigkeit der Datenschutzbehörde.

2. Bescheid vom 02.12.2021, GZ: 2021-0.845.111 (Verfahrenszahl D124.4444) Abwei-

sung einer Beschwerde, weil von Beschwerdegegner nur Mobilfunk-Nummer bekannt war und amtswegige Ermittlungen nicht zur Identifikation des Beschwerdeflegners führten

Die diesem Bescheid (nicht rechtskräftig) wurde eine Beschwerde abgewiesen, nachdem weder die Beschwerdeführerin in der Lage war, den Beschwerdegegner anders als durch eine Telefonnummer zu bezeichnen, noch amtswegige Ermittlungen ein Ergebnis erbracht hatten. Der nach der angegebenen Mobilfunk-Rufnummer zuständige Diensteanbieter hatte gegenüber der DSB eine Bekanntgabe des Inhabers der Rufnummer unter Hinweis auf die fehlende Rechtsgrundlage der Datenübermittlung abgelehnt. Auch die im Wege der Amtshilfe befasste RTR sah keine Rechtsgrundlage für die Ermittlung dieser Daten. Die behördlichen Ermittlungsmöglichkeiten waren somit erschöpft.

Damit ist die DSB als Aufsichtsbehörde ihrer Pflicht gemäß Art. 57 Abs. 1 lit. f DSGVO, sich mit einer Beschwerde zu befassen und den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen (siehe ErwGr 141 zur DSGVO) in diesem Einzelfall nachgekommen.

3. Beschwerdeverentscheidung vom 16.12.2021, GZ: 2021-0.816.492 (Verfahrenszahl D062.968)

Mit dieser Beschwerdeverentscheidung, (rechtskräftig) wurde der Beschwerde der ursprünglichen Beschwerdeführerin stattgegeben. Die DSB stellte fest, dass der ursprüngliche Beschwerdegegner, der Bundesminister für Inneres, die Beschwerdeführerin dadurch im Recht auf Auskunft verletzt hat, indem er ihr eine Auskunft nicht - wie gewünscht - per E-Mail zugestellt hat.

Der Bundesminister für Inneres (BMI) vertrat die Meinung, dass seine Auskünfte insofern heikel seien, als darin regelmäßig auch strafrechtsrelevante Daten enthalten sind. Insofern müsse eine „sichere“ Übermittlung der Auskunft gewährleistet sein, damit diese Daten nicht „in falsche Hände“ geraten. Der BMI war daher der Meinung, dass eine solche Auskunft nur postalisch und eigenhändige (RSa-Brief) gemäß § 22 AVG oder elektronisch und mit Zustellnachweis gemäß § 28 Abs. 4 ZustG zugestellt werden könne. Da es sich beim BMI um eine Behörde handle, müsse dieser das AVG und auch das ZustG anwenden.

Die DSB widersprach Letzterem nicht, sprach aber aus, dass auch das ZustG einer Zustellung per E-Mail nicht entgegensteht (§ 28 Abs. 3 iVm § 37 Abs. 1 und § 2 Z 5 ZustG) und die Zustellung einer Auskunft daher nicht zwingend gemäß § 22 AVG zu erfolgen hat. Des Weiteren sprach die DSB aus, dass der BMI neben dem AVG und dem ZustG auch das 3. Hauptstück des DSGVO anzuwenden hat. Im 3. Hauptstück des DSGVO wurde die DSRL-PJ (RL (EU) 2016/680) innerstaatlich umgesetzt, die von den für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten zuständigen Behörden, somit auch vom BMI als oberste „Sicherheitsbehörde“, anzuwenden ist. Insofern stellt das 3. Hauptstück des DSGVO in Bezug auf das AVG und das ZustG eine „lex specialis“ dar.

§ 42 Abs. 4 letzter Satz DSGVO, mit dem Art. 12 Abs. 1 der DSRL-PJ innerstaatlich umgesetzt wurde, legt nämlich als Grundsatz fest, dass der betroffenen Person die Auskunft elektronisch zu erteilen ist, wenn sie den Auskunftsantrag elektronisch gestellt hat.

Dieser Grundsatz der elektronischen Zustellung – das ist die Zustellung mit einfachem E-Mail – gilt daher auch für Auskünfte des BMI.

4. Bescheid vom 30.09.2021, GZ: 2021-0.664.183 (Verfahrenszahl D124.1865) Stattgabe einer Beschwerde, weil Verantwortlicher die Daten des Betroffenen nach erteilter Auskunft gelöscht hat

In diesem Bescheid (nicht rechtskräftig) gab die DSB der Beschwerde statt. Die DSB stellte fest, dass die Beschwerdegegnerin den Beschwerdeführer im Recht auf Auskunft verletzt hat. Der Beschwerdeführer hatte von der Beschwerdegegnerin nur die Auskunft, nicht aber auch die Löschung, seiner personenbezogenen Daten verlangt. Innerhalb eines Jahres ab Erhalt der – nach Meinung des Beschwerdeführers mangelhaften Auskunft – erhob der Beschwerdeführer Beschwerde bei der DSB. Der Beschwerdegegner hatte aber schon kurz nach Erteilung der Auskunft einen Sperrvermerk zu den personenbezogenen Daten des Beschwerdeführers gesetzt, der ua bewirkt hatte, dass ein Großteil seiner Daten gelöscht worden war.

Die DSB sprach aus, dass jeder Verantwortliche bei Auskunftserteilung gemäß Art. 15 Abs. 1 lit. f DSGVO auf das Beschwerderecht vor der DSB hinweisen muss. Dies hat in Zusammenschau mit Art. 77 DSGVO den Sinn, dass der Betroffene vor der DSB überprüfen lassen kann, ob die erteilte Auskunft mangelhaft ist. Wenn aber der Verantwortliche – wie hier – die Daten innerhalb der einjährigen Beschwerdefrist von sich aus löscht, kann der Betroffene die (behauptete Mangelhaftigkeit der) Auskunft auch nicht mehr vor der DSB überprüfen lassen. Es lag daher eine Verletzung im Recht auf Auskunft vor.

5. Bescheid vom 05.08.2021, GZ: 2021-0.301.680 (Verfahrenszahl D124.3750) Weiter Ermessensspielraum einer Behörde iZm § 5 Abs. 1 EpiG; kein Eingriff in das Recht auf Geheimhaltung

Mit Bescheid vom 5. August 2021 (rechtskräftig) hatte sich die DSB mit der Vorgehensweise einer Bezirksverwaltungsbehörde (Beschwerdegegnerin) iZm mehreren bestätigten SARS-CoV-2 Fällen an einer Schule zu befassen.

Die Infektionsfälle betrafen verschiedene Schulklassen und Stockwerke, weshalb seitens der Beschwerdegegnerin Namen, Adressen, Geburtsdaten und Mobiltelefonnummern der Schüler, Lehrpersonen sowie des Verwaltungspersonals angefordert worden waren. Diese Daten wurden in weiterer Folge in ein Webtool zur organisatorischen Abwicklung der Testungen eingespeist.

Der Beschwerdeführer, ein Schüler, der nicht als Kontaktperson zu einer positiv getesteten Person eingestuft worden war, hat infolgedessen eine SMS mit dem Angebot zu einer freiwilligen PCR-Testung erhalten. Dadurch erachtete er sich in seinem Recht auf Geheimhaltung verletzt. Die DSB wies die Beschwerde als unbegründet ab.

Die Beschwerdegegnerin stützte die Datenverarbeitung auf die in § 5 Abs. 1 EpiG enthaltene Verpflichtung und war dieser Ansicht nicht entgegenzutreten: Der Wortlaut ebendieser Bestimmung stellt unter anderem auf Krankheitsverdächtige oder Ansteckungsverdächtige ab und dient die Vorgehensweise der Ermittlung der Krankheitsquelle. Der zuständigen Behörde wird sohin ein weiter Ermessensspielraum eingeräumt, welchen die Beschwerdegegnerin gegenüberlich jedenfalls nicht überschritten hatte.

6. Bescheid vom 28.06.2021, GZ: 2021-0.417.356 (Verfahrenszahl DSB-D124.2706) Eintragung und Veröffentlichung im Ergänzungsregister für sonstige Betroffene

Mit Bescheid vom 28. Juni 2021 (nicht rechtskräftig) hatte sich die Datenschutzbehörde erstmals mit der Eintragung und Veröffentlichung natürlicher Personen im Ergänzungsregister für sonstige Betroffene (ERsB) zu befassen.

Das ERsB wird seit 2018 vom Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW) als verantwortliche Stelle geführt. Der Beschwerdeführer vertrat die Ansicht, dass seine Identität bereits aufgrund seiner Eintragung im Melderegister ausreichend feststellbar sei. Die Eintragung im ERsB mit anschließender Veröffentlichung sei daher nicht erforderlich gewesen und im Ergebnis zu Unrecht erfolgt.

Die Datenschutzbehörde überprüfte, ob eine ausreichend determinierte gesetzliche Grundlage für diesen staatlichen Eingriff vorhanden war. Dabei wurde festgehalten, dass es sich bei dem Beschwerdeführer um einen Betroffenen iSd E-GovG handelte, welchem aufgrund seiner gewerblichen Tätigkeit - abseits seiner Stellung als Privatperson - eine eigene Identität im Wirtschaftsleben zukommt. Aufgrund der gem. § 6 Abs. 1 und Abs. 4 E-GovG geforderten Differenzierung sowie der in § 16 ERegV 2009 ausdrücklich normierten Veröffentlichung erwies sich die Eintragung im Ergebnis als rechtmäßig. Die Beschwerde wegen der Verletzung im Recht auf Geheimhaltung und im Recht auf Löschung wurde abgewiesen.

7. Bescheid vom 07.07.2021, GZ 2021-0.330.691 (Verfahrenszahl D124.3524) Folgen eines Unternehmenskaufs mittels Asset-Deals auf die Rechtmäßigkeit von Direktwerbung gegenüber dem neuen Kundenstock

Mit Bescheid vom 7. Juli 2021 (nicht rechtskräftig) setzte sich die Datenschutzbehörde mit E-Mail-Newslettern auseinander, die nach dem Erwerb eines Unternehmens an die Kund_innen des erworbenen Unternehmens ohne deren Einwilligung übermittelt wurden.

Die Beschwerdegegnerin, ein Handelsunternehmen, erwarb Vermögensgegenstände eines insolventen Unternehmens, darunter auch den Goodwill und den Kundenstock, vom Masseverwalter.

Daraufhin versandte die Beschwerdegegnerin E-Mail-Newsletter zu Zwecken der Direktwerbung an die Beschwerdeführerin.

Zunächst hielt die Datenschutzbehörde fest, dass durch einen Verstoß gegen das TKG 2003 bzw. die e-Datenschutz-RL (RL 2002/58/EG) gleichzeitig eine Verletzung des Rechts auf Geheimhaltung nach § 1 Abs. 1 DSG und auch eine Verletzung jener Bestimmungen der DSGVO vorliegen kann, die dem Verantwortlichen keine zusätzlichen Pflichten iSv Art. 95 DSGVO auferlegen.

Da gemäß § 107 Abs. 3 Z 1 TKG 2003 die Zusendung elektronischer Post nur dann rechtmäßig ist, wenn der Absender die Kontaktinformation für die Nachricht im Zusammenhang mit einem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und es sich im vorliegenden Fall mangels Gesamtrechtsnachfolge bei der Beschwerdeführerin nicht um die Kundin der Beschwerdegegnerin in diesem Sinne handelt, war die Erleichterung des § 107 Abs. 3 TKG 2003 nicht einschlägig.

Die Beschwerdegegnerin hätte daher als Erwerberin des Unternehmens im Rahmen eines Asset-Deals bei den übernommenen Kunden vorab die Einwilligung zur Zusendung von Newslettern einholen müssen.

Darüber hinaus bejahte die Datenschutzbehörde ihre Zuständigkeit im gegenständlichen Verfahren trotz eines vorangegangenen UWG-Verfahrens, da weder eine Identität der Verfahrensgegenstände noch der Verfahrensparteien vorlag. Es lag daher keine Bindungswirkung des Beschlusses des OLG Graz auf den im Ergebnis abweichenden Bescheid der Datenschutzbehörde vor.

8. Bescheid vom 01.06.2021, GZ 2021-0.293.288 (Verfahrenszahl D124.3128) Betreuung einer Verkehrsstrafe durch ein Inkassobüro

Mit Bescheid vom 1. Juni 2021 (rechtskräftig) setzte sich die Datenschutzbehörde mit der Rechtmäßigkeit der Betreuung ausländischer Verkehrsstrafen durch Inkassobüros anstatt durch den im EU-VStVG normierten Weg auseinander.

Der Beschwerdeführer war im Jahr 2018 auf einer italienischen Autobahn bei einer Geschwindigkeitsübertretung „geblitzt“ worden. Die Provinz Pisa übermittelte den österreichischen Behörden daraufhin ein „Protokoll“ genanntes Schreiben, das den Beschwerdeführer zur Zahlung einer Verwaltungsstrafe aufforderte. Die österreichische Behörde übermittelte dem Beschwerdeführer das Schreiben nach völkerrechtlichen Bestimmungen, dieser verweigerte die Zahlung jedoch.

Daraufhin beauftragte die Provinz Pisa über eine italienische Gesellschaft und ein deutsches Inkassobüro ein österreichisches Inkassobüro. Dieses übermittelte mehrere Mahnungen an den Beschwerdeführer. Dabei verarbeitete die Beschwerdegegnerin zwangsläufig die personenbezogenen Daten des Beschwerdeführers.

Dies geschah unrechtmäßig und verletzte den Beschwerdeführer in seinem Recht auf Geheimhaltung, da sich die Beschwerdegegnerin auf keinen Rechtfertigungsgrund des Art. 6 DSGVO stützen konnte: Aufgrund des Umstandes, dass der (Unions-)Gesetzgeber eine bestimmte Vorgehensweise zur Eintreibung ausländischer Verwaltungsstrafen, und zwar im Wege der nationalen Vollstreckungsbehörden, normiert hat, kann die Datenverarbeitung durch die Beschwerdegegnerin als Inkassounternehmen auch durch sonstige Erlaubnistatbestände des Art. 6 DSGVO nicht gerechtfertigt werden, insbesondere kann es deshalb auch nicht zu einem Überwiegen von Interessen der Beschwerdegegnerin bzw. Dritter iSd Art. 6 Abs. 1 lit. f DSGVO kommen.

Da die Beschwerdegegnerin die personenbezogenen Daten des Beschwerdeführers unrechtmäßig verarbeitet hat, hätte sie gemäß Art. 17 Abs. 1 lit. d DSGVO dem Antrag des Beschwerdeführers auf Löschung seiner personenbezogenen Daten entsprechen müssen. Dadurch, dass sie die Löschung verweigert hat, hat sie den Beschwerdeführer auch in seinem Recht auf Löschung verletzt.

9. Bescheid vom 06.07.2021, GZ 2021-0.297.343 (Verfahrenszahl D124.3687) Kopie eines Maskenbefreiungsattests darf im Verdachtsfall an Bezirksverwaltungsbehörde und Ärztekammer zur Überprüfung übermittelt werden

Der Beschwerdeführer war im Frühjahr 2021 am Rande einer Demonstration gegen die Covid-19-Maßnahmen von Beamten der LPD Kärnten angehalten worden, weil er keine, nach § 12 der 3. COVID-19-NotMV verpflichtende, enganliegende mechanische Schutzvorrichtung getragen hatte. Der Beschwerdeführer wies daraufhin ein von einer Wiener Ärztin ausgestelltes Maskenbefreiungsattest vor. Aufgrund der Verdachtslage, dass das Attest unrechtmäßig ausgestellt worden sein könnte (die genannte Ärztin war in diesem Zusammenhang bereits mehrfach aufgefallen), übermittelten die Beamten eine Kopie an die Bezirksverwaltungsbehörde und die Ärztekammer zur Überprüfung.

Es handelte sich dabei um eine Datenverarbeitung im Sinne der §§ 1, 4, 7 und 9 des COVID-19-MG, und somit um eine Datenverarbeitung auf Basis einer gesetzlichen Grundlage im Sinne von § 4 Abs. 3 Z 2 DSGVO iVm Art. 10 DSGVO. Nach diesen Bestimmungen können die Bezirksverwaltungsbehörden und über deren Ersuchen die Organe des öffentlichen Sicherheitsdienstes im Rahmen ihrer Unterstützungspflicht gemäß § 10 COVID-19-MG die Einhaltung von Betretungsverboten, Voraussetzungen und Auflagen (wie auch das Tragen des MNS) sowie Beschränkun-

gen gemäß § 5 Abs. 4 – auch durch Überprüfung vor Ort – kontrollieren und sind weiters die Organe des öffentlichen Sicherheitsdienstes dazu verpflichtet, an Maßnahmen zur Einleitung und Sicherung eines Verwaltungsstrafverfahrens mitzuwirken. Dies ist im vorliegenden Fall rechtmäßig erfolgt.

Es konnte von Seiten der Datenschutzbehörde nicht festgestellt werden, dass die Übermittlung an die Österreichische Ärztekammer von vornherein unzulässig gewesen wäre, diente die Übermittlung doch im Ergebnis dazu, die Echtheit des medizinischen Zertifikats zu überprüfen, was wiederum für die (Nicht-)Verhängung einer Verwaltungsstrafe eine unabdingbare Voraussetzung bildete. Dadurch war die Zulässigkeit der Ermittlung aus datenschutzrechtlicher Sicht in Anlehnung an das sog. Übermaßverbot gegeben, da es denkmöglich war, dass die von der sachlich zuständigen LPD ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet waren.

Dieser Bescheid ist nicht rechtskräftig.

10. Bescheid vom 06.08.2021, GZ 2021-0.454.639 (Verfahrenszahl D124.3857) Covid-19-Antigen-Testung im Klassenverband verletzt die Schüler_innen nicht im Recht auf Geheimhaltung)

Die Beschwerdeführerinnen waren im Sommersemester 2021 Schülerinnen an einer Volksschule und einer Mittelschule. Als Voraussetzung für die Teilnahme am Präsenzunterricht an beiden Schulen wurde ein Covid-19-Eintritts-Selbsttest oder ein anderer Nachweis einer geringen epidemiologischen Gefahr verlangt. Die Durchführung der Selbsttests erfolgte im Klassenverband unter Kontrolle der anwesenden Lehrkraft. Bei Verweigerung des Selbsttests und der Erbringung eines (alternativen) Nachweises einer geringen epidemiologischen Gefahr wurde die Teilnahme am Präsenzunterricht verweigert. Die Testergebnisse wurden nicht laut vorgelesen und die Nachweise der Beschwerdeführerinnen nicht an Dritte übermittelt.

Soweit sich die Beschwerde gegen den Bundesminister für Bildung, Wissenschaft und Forschung, die Stadtgemeinde sowie gegen das Lehrpersonal richtete, war sie schon deshalb abzuweisen, weil diese im gegenständlichen Fall nicht als Verantwortliche der Datenverarbeitung nach Art. 4 Z 7 DSGVO in Betracht kamen. Sie entschieden weder über Mittel noch über Zwecke der Datenverarbeitung. Eine Zusammenschau von § 35 mit der Anlage B der C-SchVO 2020/21 ergibt, dass in die gegenständliche Datenverarbeitung lediglich die Bildungsdirektion Salzburg und die Schulleitungen involviert waren und daher auch nur diese definitionsgemäß als Verantwortliche und damit Beschwerdegegner in Betracht kommen.

Vor dem Hintergrund all dieser Überlegungen kam die Datenschutzbehörde daher zu dem Ergebnis, dass die hier relevante Datenverarbeitung auf die in § 44 SchUG iVm § 35 C-SchVO 2020/21 normierte gesetzliche Verpflichtung der Lehrkräfte, zur Sicherheit der Schüler in der Schule sowie zur Ermöglichung eines ordnungsgemäßen Schulbetriebes, Nachweise über deren geringe epidemiologische Gefahr zu erheben, gestützt werden konnte und das gelindeste Mittel darstellte. Es lag somit eine rechtmäßige Datenverarbeitung nach Art. 9 Abs. 2 lit. i DSGVO vor.

Die hier relevante Datenweitergabe erwies sich daher als rechtmäßig und war von keiner Verletzung im Recht auf Geheimhaltung der Beschwerdeführerinnen auszugehen.

Dieser Bescheid ist nicht rechtskräftig.

11. Bescheid vom 10.06.2021, GZ 2021-0.404.151 (Verfahrenszahl D124.4082) Unerlaubte Einsichtnahme in den elektronischen Impfpass

Im Bescheid vom 10. Juni 2021 (nicht rechtskräftig) hatte sich die DSB mit dem Vorwurf der unerlaubten Einsichtnahme einer Ärztin in den elektronischen Impfpass einer Betroffenen zu befassen.

Die Beschwerdegegnerin ist niedergelassene Ärztin und betreibt eine Ordination. Die Beschwerdegegnerin und die Beschwerdeführerin sind einander bekannt, da die Schwägerin der Beschwerdeführerin Mitarbeiterin der Beschwerdegegnerin ist. Die Mitarbeiterin der Beschwerdegegnerin teilte der Beschwerdegegnerin mit, dass am Wochenende eine Familienfeier geplant sei. Daraufhin nahm die Beschwerdegegnerin in den elektronischen Impfpass zu Daten der Beschwerdeführerin Einsicht. Rechtfertigend führte die Beschwerdegegnerin aus, dass es ihr seit Beginn der Pandemie gelungen sei, Covid-19 Infektionen aus der Ordination fern zu halten. Nachdem mittlerweile bekannt sei, dass gehäuft Cluster nach Familienfeiern auftreten, habe sie für sich und ihre Mitarbeiterin durch die Abfrage des Impfpasses eine Risikoabschätzung durchgeführt. Die Beschwerdegegnerin stützte sich daher auf ein überwiegendes berechtigtes Interesse.

Bei den eingesehenen Daten handelt es sich jedoch um Gesundheitsdaten gemäß Art. 4 Z 15 DSGVO. Diese gelten gemäß Art. 9 Abs. 1 DSGVO als besondere Kategorie personenbezogener Daten und dürfen ausschließlich in den in Abs. 2 DSGVO genannten Fällen verarbeitet werden. Im Vergleich zu den Rechtfertigungstatbeständen des Art. 6 Abs. 1 DSGVO fehlen die Zulässigkeitstatbestände der „Verarbeitung im berechtigten Interesse des Verantwortlichen oder eines Dritten“ (Art. 6 Abs. 1 lit. f DSGVO) und der „Verarbeitung zur Vertragserfüllung“ (Art. 6 Abs. 1 lit. b DSGVO).

Da der in Art. 6 Abs. 1 lit. f DSGVO befindliche Rechtfertigungsgrund nicht von Art. 9 Abs. DSGVO umfasst ist, war die Berufung auf diesen Grund konsequenterweise unzulässig. Der Beschwerde wurde daher stattgegeben und es wurde festgestellt, dass die Beschwerdeführerin in ihrem Recht auf Geheimhaltung verletzt wurde.

12. Bescheid vom 22.02.2021, GZ 2021-0.119.956 (Verfahrenszahl D124.1965) Das Recht auf Auskunft (Art. 15 DSGVO) umfasst zwar nicht die Übersendung von Akten, jedoch ein Recht auf die Beauskunftung der gesundheitsbezogenen Daten in Patientenakten

Die Beschwerdeführerin erhob Beschwerde gegen die Stadt Wien (als Trägerin einer Krankenanstalt), vertreten durch die MA 63, und behauptete, im Recht auf Auskunft verletzt zu sein, da ihr ihre gesundheitsbezogenen Daten (Patientenakten, Diagnosen, Untersuchungsergebnisse etc.) aus ihren Krankenhausaufenthalten nicht beauskunftet wurden. Die Beschwerdeführerin berief sich insbesondere auf ErwG. 63, 2. Satz DSGVO. Die Beschwerdegegnerin führte aus, dass nach der DSGVO kein Recht bestehe, alle Patientenakten vollinhaltlich als Kopie zu übermitteln. Darüber hinaus sei eine Kopie der Krankengeschichte gegen Kostenersatz gemäß § 17a Abs. 2 lit. g Wr. KAG möglich. Art. 15 DSGVO werde von den spezielleren Rechten aus dem Wr. KAG verdrängt, welche ihre europarechtlichen Fundierungen in der RL 2011/24/EU haben. Die Datenschutzbehörde gab der Beschwerde statt und stellte eine Verletzung im Recht auf Auskunft fest, da sich in der Auskunft der Beschwerdegegnerin lediglich die Namen der Akten/Befunde und Therapien mit Datum befanden. Aus Art. 15 iVm. ErwGr. 63 2 Satz DSGVO lasse sich zwar kein Anspruch auf (kostenfreie) Herausgabe ganzer Dokumente ableiten, jedoch ein Anspruch auf die gesundheitsbezogenen Daten in Patientenakten, also Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen.

Im Übrigen derogiert § 17a Abs. 2 lit. g Wr. KAG dem Art. 15 DSGVO nicht, da die RL 2011/24/EU auf die RL 95/46/EG (nunmehr DSGVO) verweist, welche für die Verarbeitung personenbezogener Daten maßgeblich ist und das Wr. KAG kein spezielleres Auskunftsrecht ohne Kostenersatz normiert.

Dieser Bescheid ist rechtskräftig.

**13. Bescheid vom 11.03.2021, GZ 2021-0.017.641 (Verfahrenszahl D124.2337)
Überschießende Akteneinsicht im Rahmen eines Ermittlungsverfahrens der
Staatsanwaltschaft**

Mit Bescheid vom 11. März 2021 (nicht rechtskräftig) bejahte die Datenschutzbehörde abermals ihre Zuständigkeit gegenüber Staatsanwaltschaften und führte weitergehend aus, dass auch die einfachgesetzlichen Bestimmungen der StPO im Lichte der Verfassungsbestimmung des § 1 DSG sowie der unionsrechtlichen Datenminimierungspflicht auszulegen seien.

Ausgangspunkt des Beschwerdeverfahrens war ein einheitlich geführtes Ermittlungsverfahren, im Rahmen dessen die zuständige Staatsanwaltschaft dem Zweitbeschuldigten antragsgemäß vollständige Akteneinsicht (§ 51 StPO) gewährte. Dies beinhaltete unter anderem ein medizinisches Gutachten, welches aufgrund eines der Erstbeschuldigten vorgeworfenen Körperverletzungsdeliktes erstellt worden war, dabei jedoch in keinerlei sachlichem Zusammenhang mit der Tat des Zweitbeschuldigten stand. Die Datenschutzbehörde gab der infolgedessen erhobenen Beschwerde der Erstbeschuldigten wegen Verletzung im Recht auf Geheimhaltung statt und führte begründend aus, dass auch Datenverarbeitungen durch zuständige Strafverfolgungsbehörden ungeachtet einer gesetzlichen Grundlage stets auf ihre Verhältnismäßigkeit (Datenminimierungspflicht) zu prüfen seien.

14. Bescheid vom 08.09.2020, GZ 2020-0.436.002 (Verfahrenszahl D124.909) Einstufungen von Betroffenen in Geo Milieus zum Zwecke des strategischen Marketings sind Profiling iS von Art. 4 Z 4 DSGVO. Eine Auskunftserteilung hat gemäß Art. 15 Abs. 1 lit. h DSGVO zu erfolgen und sollte die Eingangsvariablen, deren Gewichtung und eine Erklärung, weshalb Betroffenen ein bestimmtes Bewertungsergebnis zugeordnet wird, oder gleichwertige Informationen beinhalten, um dem Betroffenen die Rechte auf Richtigstellung und Löschung zu ermöglichen

Im Bescheid vom 8. September 2020 (rechtskräftig) hatte sich die Datenschutzbehörde mit dem Umfang eines Auskunftsanspruchs im Rahmen der sogenannten Geo_Milieus auseinanderzusetzen. Geo_Milieus sind, vereinfacht gesprochen, Einstufungen von Personen, basierend auf einer Wahrscheinlichkeitsrechnung zum Zwecke des strategischen Marketings. Derartige Einstufungen sind u.a. „Wahrscheinlichkeitswert_konservative“ (beschrieben als „Stark von christlichen Wertvorstellungen geprägt, hohe Wertschätzung von Bildung und Kultur, kritisch gegenüber aktuellen gesellschaftlichen Entwicklungen“) oder „Wahrscheinlichkeitswert_hedonisten“ (beschrieben als „Die momentbezogene, erlebnishungrige untere Mitte: Leben im Hier und Jetzt, Suche nach Spaß und Unterhaltung; Verweigerung von Konventionen der Mehrheitsgesellschaft“).

Der Beschwerdeführer hatte zwar Auskunft zu den - ihm zugeordneten - Wahrscheinlichkeitswerten und den Beschreibungen der zugeordneten Geo_Milieus erhalten, jedoch keine Angaben darüber, aufgrund welcher Parameter bspw. der „Wahrscheinlichkeitswert_konservative“ bei ihm 2,03% und der Wahrscheinlichkeitswert_hedonisten 9,28 % betrug. Der Beschwerdeführer relevierte daher eine unvollständige Auskunft, da der Adressverlag unter Berufung auf Betriebs- und Geschäftsgeheimnisse sich weigerte, nähere Auskunft zur Errechnung der Werte zu erteilen.

Die Datenschutzbehörde stellte zunächst fest, dass es sich bei Errechnung und Zuordnung der Geo_Milieus Wahrscheinlichkeiten um ein Profiling gemäß Art. 4 Z 4 DSGVO handelt, da im Rahmen einer automatisierten Verarbeitung insbesondere Aspekte bezüglich wirtschaftlicher Lage, persönlicher Vorlieben und Interessen eines Betroffenen analysiert, segmentiert und diesbezügliche Wahrscheinlichkeitswerte errechnet wurden. Da Art. 15 Abs. 1 lit. h DSGVO vorsieht, dass bei Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zu erteilen sind, weiters Art. 15 Abs. 1 lit. h DSGVO die spezifischen Auskunftsrechte nicht abschließend auf Art. 22 Abs. 1 und 4 DSGVO beschränkt, sondern diese Rechte durch das Wort zumindest („at least“) auch auf andere Fälle ausgedehnt sehen will, hat die Datenschutzbehörde eine Auskunftserteilung zum Zustandekommen der Geo_Milieus gemäß Art. 12 Abs.1 iVm 15 Abs. lit. h DSGVO angeordnet. Es ist Betroffenen nur durch eine Auskunftserteilung der Eingangsvariablen, deren Gewichtung und einer Erklärung, weshalb Betroffenen letztlich ein bestimmtes Bewertungsergebnis zugeordnet wird, möglich, dass diese ihre Betroffenenrechte auf Richtigstellung und Löschung wahrnehmen können.

Demgegenüber treten auch Geschäfts- und Betriebsgeheimnisse des Adressverlages in den Hintergrund, da die im Verfassungsrang (§ 1 Abs. 3 DSG) stehenden bzw. auf EU-Primärrecht (Art. 8 EU-GRC) basierenden Rechte auf Auskunft und Richtigstellung gewichtiger zu bewerten und Ausnahmen von den allgemeinen Bestimmungen der DSGVO eng auszulegen sind (vgl. EuGH C-311/18). Das Begehren auf Offenlegung der vollständigen Berechnungsmethodik – wie vom Beschwerdeführer ebenfalls verlangt – wurde hingegen abgewiesen. Art. 15 Abs. 1 lit. h DSGVO spricht lediglich von „aussagekräftigen Informationen zur involvierten Logik und deren Auswirkungen“, nicht aber von der involvierten Logik selbst.

15. Bescheid vom 16.04.2021, GZ 2021-0.258.447 (Verfahrenszahl DSB-D124.2651) Entfernung des Personenbezugs als Mittel zur Löschung

Mit Bescheid vom 16. April 2021 (nicht rechtskräftig) hatte sich die Datenschutzbehörde mit einer Beschwerde gegen eine Immobilitätentreuhänderin wegen einer Verletzung im Recht auf Löschung auseinandersetzen.

Der Beschwerdeführer hatte mehrfach die Löschung seiner Daten begehrt, da er keine weiteren Zusendungen von der Beschwerdegegnerin erhalten wollte. Die Beschwerdegegnerin änderte dessen Namen in ihrer Personendatenbank auf Max Mustermann, ersetzte seine Anschrift mit einem Platzhalter, fügte zur Adresse einen Vermerk ein, wonach zu dieser Liegenschaft kein Grundbuchauszug mehr einzuholen sei und löschte sämtliche Korrespondenz mit diesem. Die Beschwerdegegnerin wandte sich jedoch neuerlich mit einem Schreiben zwecks Liegenschaftsakquise an den Beschwerdeführer.

Die DSGVO enthält keine Definition des Begriffs von Löschung iSv Art. 17 DSGVO und kommt die Entfernung des Personenbezugs grundsätzlich als Mittel zur Löschung in Betracht, jedoch muss eine Identifizierbarkeit auch unter Heranziehung zusätzlicher Mittel ausgeschlossen sein (vgl. ErwGr 26 DSGVO). Dies war gegenständlich nicht gegeben, konnte doch durch eine Grundbuchabfrage der Personenbezug wiederhergestellt werden. Überdies befand die Datenschutzbehörde die wiederholte Kontaktaufnahme zur Liegenschaftsakquise im Lichte ihrer Rsp als unrechtmäßig, weshalb der Tatbestand des Art. 17 Abs. lit. d DSGVO als erfüllt zu betrachten war und der Beschwerde stattgegeben wurde.

**16. Bescheid vom 02.02.2021, GZ 2020-0.844.057 (Verfahrenszahl: DSB-D124.733)
Verletzung im Recht auf Geheimhaltung: Bonitätsabfrage ohne konkreten Grund
für einen Verdacht eines Versicherungsbetruges im Zuge der Bearbeitung eines
Schadensfalles**

Im Bescheid vom 2. Februar 2021 (rechtskräftig) hatte sich die Datenschutzbehörde mit einer Beschwerde wegen behaupteter Verletzung im Recht auf Geheimhaltung (§ 1 DSG) und einer Interessensabwägung aufgrund von berechtigten Interessen (Art. 6 Abs. 1 lit. f DSGVO) auseinander zu setzen.

Die Beschwerdeführerin erlitt einen Unfall, welcher an die zuständige Haftpflichtversicherung (Beschwerdegegnerin) gemeldet wurde. Diese prüfte den Schadensfall unter anderem dadurch, indem sie eine Abfrage bei einer Bonitätsdatenbank zur Zahlungsmoral der Beschwerdeführerin tätigte. Dabei wurde auf eine bereitgestellte Ampelfunktion über eine entsprechende Schnittstelle zurückgegriffen. Im konkreten Fall wurde die Ampelfarbe „rot“ angezeigt, was eine negative Zahlungsmoral bedeutete.

Die Beschwerdegegnerin begründete die gegenständliche Verarbeitung damit, dass diese auf Basis von berechtigten Interessen der Beschwerdegegnerin und ihrer Gläubiger an der Bekämpfung von Versicherungsbetrug zulässig gewesen sei. Da eine Korrelation zwischen der Zahlungsmoral der Betroffenen und der Anfälligkeit für Versicherungsbetrug bestehe, habe die Beschwerdegegnerin im Verdachtsfall die gegenständliche Bonitätsdatenabfrage zur Zahlungsmoral getätigt.

Im laufenden Verfahren hat die Beschwerdegegnerin es aber unterlassen, einen konkreten Grund für ihren Verdacht, die Beschwerdeführerin könnte ein Risiko für Versicherungsbetrug sein, darzulegen und konnte daher nicht nachvollziehbar vorbringen, warum ihre wirtschaftlichen Interessen in diesem Fall gegenüber den Interessen der Beschwerdegegnerin überwiegen, zumal die Beschwerdegegnerin der Beschwerdeführerin die gegenständliche Versicherungsleistung ausgezahlt hat. Der Beschwerde wurde stattgegeben.

17. Bescheid vom 15.02.2021, GZ 2021-0.101.211 (Verfahrenszahl D124.3158) Übermittlung eines negativen PCR-Testergebnisses an das Gesundheitsamt

Mit Bescheid vom 15. Februar 2021 (rechtskräftig) setzte sich die Datenschutzbehörde mit der datenschutzrechtlichen Zulässigkeit der Übermittlung eines negativen PCR-Testergebnisses an eine Bezirksverwaltungsverwaltungsbehörde (als Gesundheitsamt) auseinander.

Der Beschwerdeführer hat einen freiwilligen PCR-Test (SARS-CoV-2) bei der Beschwerdegegnerin (Betreiberin eines Labors) durchgeführt. Das Testergebnis war negativ. In weiterer Folge hat der Beschwerdeführer in Erfahrung gebracht, dass die Beschwerdegegnerin das negative Testergebnis an das zuständige Gesundheitsamt übermittelt hat, was nach Auffassung des Beschwerdeführers unrechtmäßig erfolgt sei.

Grundlegend war zu überprüfen, ob die Information über ein negatives PCR-Testergebnis einer bestimmten Person in den Schutzbereich von Art. 9 DSGVO fällt. Festzuhalten war, dass die Legaldefinition „Gesundheitsdaten“ des Art. 4 Z 15 DSGVO nicht an eine gewisse (Mindest-) Beeinträchtigung der körperlichen oder geistigen Gesundheit anknüpft. Noch deutlicher wird dies in ErwGr. 35 der Verordnung, wonach zu den personenbezogenen Gesundheitsdaten alle Daten zählen sollten, aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Auch der EuGH legt den Begriff „Gesundheitsdatum“ weit aus (vgl. zur insofern vergleichbaren Rechtslage nach der Richtlinie 95/46 das Urteil des EuGH vom 6. November 2003, C-101/01, Rs

Lindqvist, Rz 50 f). Somit war für die Beurteilung der hier relevanten Datenübermittlung (auch) das Schutzregime von Art. 9 Abs. 2 DSGVO zu beachten.

Im Hinblick auf die Rechtmäßigkeit war festzuhalten, dass sich aus Art. 9 Abs. 1 lit. i DSGVO iVm § 3 Abs. 1 Z 1, Z 1a sowie Abs. 2 EpiG keine Verpflichtung zur Abgabe einer behördlichen Meldung über einen negativen PCR-Test ergibt. Allerdings kann die Pflicht zur Abgabe einer behördlichen Meldung gemäß § 1 Abs. 2 EpiG durch den Bundesminister für Gesundheit dann erweitert werden, wenn dies aus epidemiologischen Gründen gerechtfertigt oder auf Grund internationaler Verpflichtungen erforderlich ist. Von dieser Möglichkeit zur Erweiterung der Meldepflichten wurde im Rahmen der aktuellen Pandemie Gebrauch gemacht. So wurde § 1 Abs. 3 der Verordnung des Bundesministers für Gesundheit betreffend elektronische Labormeldungen in das Register anzeigepflichtiger Krankheiten, BGBl. II Nr. 184/2013 idGF, dahingehend geändert, dass gemäß dessen § 1 Abs. 3 Einrichtungen dazu verpflichtet sind, im Falle einer Pandemie mit COVID-19 auch alle negativen und ungültigen Ergebnisse an die Bezirksverwaltungsbehörde zu übermitteln.

Die hier relevante Verordnung, mit der die Meldepflicht erweitert wurde, beruht auf der gesetzlichen Grundlage des § 3 Abs. 1 EpiG und bindet die jeweiligen medizinischen Einrichtungen gleichermaßen. Zudem muss nach ErwGr. 41 erster Satz DSGVO eine Rechtsgrundlage, auf die (der hier relevante) Art. 9 Abs. 2 lit. i DSGVO abgestellt, auch nicht notwendigerweise auf einem von einem Parlament angenommenen Gesetzgebungsakt beruhen. Ferner handelt es sich bei einem PCR-Test (also der Erhebung, ob eine Person infiziert ist) um keinen besonderen Datenverarbeitungsvorgang – wie etwa Profiling gemäß Art. 4 Z 4 DSGVO – sodass auch nicht davon auszugehen ist, dass der in Art. 9 Abs. 2 lit. i DSGVO der Verordnung enthaltene Maßstab an nationale Vorschriften, „angemessene und spezifische Schutzmaßnahmen“ zu normieren, verletzt wäre.

Die Erweiterung der Meldepflicht des § 3 Abs. 1 EpiG ist zur Bekämpfung von COVID-19 auch zweckdienlich, da das Datenmaterial (also länder- und bundesspezifische Informationen über negative und ungültige PCR-Tests) relevant für die Ausrichtung der Pandemiestrategie – insbesondere der Teststrategie – ist.

Die Datenschutzbehörde gelangte daher zu dem Ergebnis, dass auch die Übermittlung eines negativen PCR-Testergebnisses an eine Bezirksverwaltungsbehörde (als Gesundheitsamt) zulässig ist.

18. Bescheid vom 09.03.2021, GZ 2021-0.157.107 (Verfahrenszahl D124.2924) Gesundheitsfragebogen über eine mögliche Infektion mit dem Coronavirus (SARS-CoV-2)

Mit Bescheid vom 9. März 2021 (nicht rechtskräftig) setzte sich die Datenschutzbehörde mit der Frage auseinander, ob es datenschutzrechtlich zulässig ist, einen Gast dazu anzuhalten, einen Fragebogen zur Ermittlung seines gesundheitlichen Zustandes auszufüllen, bevor er sich in einem Hotel aufhalten darf.

Der Beschwerdeführer hat einen Aufenthalt im Hotel der Beschwerdegegnerin gebucht. Der Beschwerdeführer wurde beim Betreten des Hotels aufgefordert, einen physischen Fragebogen auszufüllen. Der Fragebogen wurde laut Angabe der Beschwerdegegnerin „zur Reduzierung des Risikos von Infektionskrankheiten“ im Zusammenhang mit dem Coronavirus eingesetzt. Es wurden Symptome abgefragt, die nach aktueller wissenschaftlicher Evidenz mit dem Coronavirus in Verbindung stehen. Der Beschwerdeführer hat diesen Fragebogen allerdings nicht ausgefüllt, sondern durchgestrichen. Somit wurden auch keine Daten von ihm erhoben.

Ausgehend von diesem Sachverhalt war festzuhalten, dass Voraussetzung für die Erhebung einer Beschwerde an die Datenschutzbehörde eine Datenverarbeitung ist (vgl. Art. 4 Z 1 DSGVO) und durch die erfolgte Datenverarbeitung eine Verletzung in Rechten behauptet wird. Geplante, jedoch letztlich nicht erfolgte Datenverarbeitungen sind einer Beschwerde nach Art. 77 DSGVO iVm § 24 DSG nicht zugänglich. Dies legt bereits der Wortlaut von Art. 77 Abs. 1 DSGVO und § 24 Abs. 1 DSG nahe, wonach eine Beschwerde dann erhoben werden kann, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (und nicht „verstoßen wird“ oder „verstoßen könnte“).

Eine nachprüfende Kontrolle durch die Datenschutzbehörde und die Gerichte trägt auch dem Umstand Rechnung, dass ein Beschwerdeverfahren der Geltendmachung subjektiver Rechte dient. Somit ist es grundlegende Voraussetzung, dass die Rechtsposition der betroffenen Person durch ein Fehlverhalten des Verantwortlichen unmittelbar beeinträchtigt wird oder wurde. Ein Beschwerdeverfahren dient jedoch nicht dem Zweck, die Einhaltung objektiver Pflichten durch einen Verantwortlichen zu überprüfen, ohne dass sich die Nichteinhaltung in einer Beeinträchtigung subjektiver Rechtspositionen manifestiert (vgl. zu Datensicherheitsmaßnahmen den Bescheid vom 13. September 2018, GZ: DSB-D123.070/0005-DSB/2018). Der Beschwerdeführer brachte auch nicht vor, dass das Nichtausfüllen des Fragebogens mit einem Nachteil für diesen verbunden wäre (wie etwa die Weigerung der Beschwerdegegnerin, einen Beherbergungsvertrag abzuschließen).

Die Beschwerde war im Ergebnis abzuweisen.

19. Bescheid vom 3. Mai 2021, GZ 2021-0.285.169 (Verfahrenszahl D124.3448) Keine Anwendung des DSG und der DSGVO auf ausschließlich persönliche oder familiäre Tätigkeiten – „Haushaltsausnahme“

Mit verfahrenseinleitender Eingabe behauptete der Beschwerdeführer eine Verletzung im Recht auf Geheimhaltung durch die Beschwerdegegnerin (seine Ex-Frau) und brachte zusammengefasst vor, dass die Beschwerdegegnerin einen Gerichtsbeschluss mit seinen sensiblen Gesundheitsdaten mittels WhatsApp an eine dritte Person weitergegeben habe.

Die Beschwerdegegnerin teilte im Verfahren vor der Datenschutzbehörde hierzu mit, dass es sich bei der dritten Person um die Mutter des Beschwerdeführers bzw. ihre ehemalige Schwiegermutter handeln würde und die verfahrensgegenständliche Übermittlung allein aus der Sorge um die Betreuung des gemeinsamen Sohns erfolgt wäre.

Die Datenschutzbehörde wies die Beschwerde unter Verweis auf die Bestimmung des Art. 2 Abs. 2 lit. c DSGVO (umgangssprachlich auch bezeichnet als „Haushaltsausnahme“) ab und verwies darauf, dass die verfahrensgegenständliche Verarbeitung zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgte, weshalb der Anwendungsbereich der DSGVO bzw. des DSG nicht eröffnet war.

Dieser Bescheid ist rechtskräftig.

20. Bescheid vom 20. Juli 2021, GZ 2020-0.128.590 (Verfahrenszahl D124.1700) Übermittlung eines öffentlich zugänglichen Videos

Die Beschwerdeführerin behauptete in ihrer Beschwerde vom Beschwerdegegner in ihrem Recht auf Geheimhaltung verletzt worden zu sein. Erklärend führte die Beschwerdeführerin hierzu aus, dass im Internet ein Video hinsichtlich eines von ihr getätigten Interviews kursiere, in welchem sie sich zu den Themen „Ausländer“ und „Asyl“ geäußerte habe. Der Beschwerde-

gegner habe über seine dienstliche E-Mail-Adresse an einen Verteiler von insgesamt 234 E-Mail-Adressen den Link zu diesem Video übermittelt.

Der Beschwerdegegner zog sich auf den Standpunkt zurück, dass das Video mit dem Interview öffentlich zugänglich sei, weshalb auch keine Verletzung im Recht auf Geheimhaltung vorliegen könne.

Die Datenschutzbehörde verwies in ihrem Bescheid zunächst darauf, dass die generelle Annahme des Nichtvorliegens einer Verletzung schutzwürdiger Geheimhaltungsinteressen für zulässigerweise veröffentlichte Daten nicht mit den Bestimmungen der DSGVO vereinbar ist, weshalb es für die Verarbeitung der gegenständlichen Daten auch einer entsprechenden Rechtfertigung im Sinne des § 1 Abs. 2 DSG, Art. 6 Abs. 1 bzw. Art. 9 DSGVO bedarf.

Da aufgrund der Aussagen der Beschwerdeführerin im Interview auf ihre politische Meinung bzw. weltanschauliche Überzeugung geschlossen werden konnte und es sich daher um sensible Daten bzw. eine „besondere Kategorie“ von Daten gemäß Art. 9 Abs. 1 DSGVO handelt, war der Versand der E-Mail bzw. die Übermittlung der Daten anhand des Art. 9 DSGVO zu prüfen.

In Ermangelung eines tragenden Eingriffstatbestandes gemäß § 1 Abs. 2 DSG und Art. 9 DSGVO wurde der Beschwerde stattgegeben und ausgesprochen, dass der Beschwerdegegner durch den Versand des Interviews an 234 E-Mail-Adressaten die Beschwerdeführerin in ihrem Recht auf Geheimhaltung verletzte.

Dieser Bescheid ist rechtskräftig.

21. Bescheid vom 6. August 2021, GZ: 2021-0.515.231 (Verfahrenszahl D124.3897) Recht auf Berichtigung, Führung von akademischen Titeln

Der Beschwerdeführer behauptete in seiner Beschwerde eine Verletzung im Recht auf Berichtigung und brachte begründend vor, die Beschwerdegegnerin, seine Wohnortsgemeinde, habe amtswegig, ohne seine Zustimmung die Löschung der bisher zu ihm im Melde- und Personenstandsregister eingetragenen Standesbezeichnungen „Ing.“, „EUR ING“ sowie den akademischen Grad „DI (FH)“ veranlasst und diese durch die Eintragung „Dipl. -HTL-Ing.“ ersetzt. Seinem Antrag auf Berichtigung der ihn betreffenden Einträge sei von der Beschwerdegegnerin jedoch nicht entsprochen worden.

Die Datenschutzbehörde stellte zunächst fest, dass der Beschwerdeführer zur Führung des Titels „Diplom -HTL-Ingenieur“, in der abgekürzten Form „Dipl.-HTL-Ing.“, berechtigt ist. Da der Antrag des Beschwerdeführers aber darauf gerichtet war, den Titel „Diplom -HTL-Ingenieur“ durch den akademischen Grad „DI (FH)“ sowie durch die Standesbezeichnung „Ing.“ zu ersetzen sowie um die Bezeichnung „EUR ING“ zu ergänzen, wies die Datenschutzbehörde darauf hin, dass Art. 16 DSGVO nicht das Recht zu entnehmen ist, eine Bezeichnung durch einen von einer Fachhochschule verliehenen akademischen Grad bzw. durch eine Standesbezeichnung ersetzen zu lassen.

Da der Beschwerdeführer im Verfahren vor der Datenschutzbehörde auch nicht nachweisen konnte, dass er zur Führung des akademischen Grades „DI (FH)“ überhaupt berechtigt ist und für die Bezeichnung „EUR ING“ weder eine gesetzliche Grundlage im Ingenieurgesetz 2017, noch im Nationalen Qualifikationsrahmen-Gesetz besteht, wurde die Beschwerde abgewiesen.

Dieser Bescheid ist nicht rechtskräftig.

**22. Bescheid vom 07. Jänner 2021, GZ: 2020-0.816.655 (Verfahrenszahl D124.2399)
Teilweise Stattgabe der Beschwerde, weil über Rechtsgrundlage im Rahmen der zu erteilenden Information nicht informiert wurde; Information muss nicht in Landessprache der Beschwerdeführerin erteilt werden**

Mit diesem Bescheid (rechtskräftig) gab die DSB der Beschwerde einer Beschwerdeführerin statt, die ihren Aufenthaltsort offenbar in Polen hatte, aber ihre Datenschutzbeschwerde direkt bei der österreichischen DSB einbrachte. Inhaltlich ging es darum, dass der Beschwerdegegner - ein österreichischer Verantwortlicher - die Kontaktdaten der Beschwerdeführerin bei einem Unternehmen X angefragt hatte, das der Beschwerdeführerin zuvor Fenster verkauft hatte. Die Kontaktdaten der Beschwerdeführerin verwendete die Beschwerdegegnerin, deren Unternehmensgegenstand die Herstellung von Fensterbeschlägen ist, um der Beschwerdeführerin in einem Schreiben ua mitzuteilen, dass die beim Unternehmen X gekauften Fenster möglicherweise fehlerhafte Fensterbeschläge aufweisen würden. Das Schreiben war in polnischer Sprache verfasst. Die Beschwerdeführerin brachte daraufhin Beschwerde bei der DSB ein und machte die verletzten Informationspflichten der Beschwerdegegnerin gemäß Art. 14 DSGVO geltend. Die Beschwerdegegnerin erteilte der Beschwerdeführerin im laufenden Verfahren keine „Information“, sondern eine „Auskunft nach Art. 15 DSGVO“. Die DSB sprach aus, dass die Informationspflichten prinzipiell auch durch eine Auskunftserteilung im Sinne des Art. 15 DSGVO erfüllt werden könnten. Im vorliegenden Fall hätte die Beschwerdegegnerin der Beschwerdeführerin aber die Rechtsgrundlage der Datenverarbeitung nicht mitgeteilt, wozu die Beschwerdegegnerin aber gemäß Art. 14 Abs. 1 lit. c DSGVO verpflichtet sei.

Die Beschwerdeführerin war der Ansicht, dass die erteilte „Auskunft“ in polnischer Sprache erfolgen müsse, da auch beide Schreiben der Beschwerdegegnerin – die Anfrage um die Kontaktdaten der Beschwerdeführerin ans Unternehmen X sowie der Brief an die Beschwerdeführerin - auf Polnisch erfolgt seien. Dazu sprach die DSB aus, dass sie die Beschwerdeführerin, deren Aufenthaltsort sich in Polen befinde, darauf aufmerksam gemacht habe, dass sie ihre Beschwerde im Rahmen des One-Stop-Shops bei der polnischen Aufsichtsbehörde einbringen könne, die Beschwerdeführerin dies aber abgelehnt habe. Die Beschwerdeführerin führte nicht an, dass sie die ihr erteilten Informationen (sprachlich) nicht erfassen konnte, weshalb die „Auskunft“ auf Deutsch zulässig gewesen wäre.

23. Bescheid vom 22. Jänner 2021, DSB-D124.1177/0006-DSB/2019 § 2f Abs. 1 Z 6 lit. a FOG iVm Art. 9 Abs. 2 lit. j DSGVO erlaubt die Verarbeitung der politischen Hintergrundinformation

Der Beschwerdeführer verlangte von der Beschwerdegegnerin, der Stiftung Dokumentationsarchiv des österreichischen Widerstandes (kurz: DÖW), die Löschung seiner personenbezogenen Daten, die für Zwecke des so genannten „Schnittarchivs“ verarbeitet werden. Die Datenschutzbehörde sprach hier aus, dass die Beschwerde abgewiesen wird. Einerseits ist die Verarbeitung personenbezogener Daten des Beschwerdeführers, und zwar auch die politische Hintergrundinformation zu seiner Person, durch eine nationale Rechtsgrundlage – nämlich § 2f Abs. 1 Z 6 lit. a FOG – gemäß Art. 9 Abs. 2 lit. j DSGVO gerechtfertigt. Darüber hinaus liegt auch kein wirksamer Widerspruch des Beschwerdeführers gemäß Art. 21 Abs. 6 DSGVO vor. Der Verantwortliche - hier: das DÖW - kann gemäß Art. 21 Abs. 6 den Widerspruch aber ablehnen, wenn die Verarbeitung zu wissenschaftlichen, historischen oder statistischen Zwecken zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist. Ein solches öffentliches Interesse war aber durch die erlaubte Verwendung der Daten zu im öffentlichen Interesse liegenden Archivzwecken gemäß § 2f Abs. 1 Z 6 lit. a FOG gegeben. Die Beschwerde war daher abzuweisen.

Dieser Bescheid ist rechtskräftig.

Österreichische Post AG

Mit Erkenntnis vom 14. Dezember 2021, Ro 2021/04/0007-4, wies der Verwaltungsgerichtshof die Revision der Österreichischen Post im Ergebnis ab und bestätigte somit letztinstanzlich die mittlerweile mehrjährige Spruchpraxis der DSB, wonach bereits die Zuordnung einer (bloß) vermuteten politischen Meinung („Parteiaffinität“) gegen das Verarbeitungsverbot des Art. 9 DSGVO verstößt.

Diese nun auch vom Verwaltungsgerichtshof vertretene Rechtsansicht wurde bereits zuvor sowohl durch das Bundesverwaltungsgericht (Erkenntnis vom 20. Mai 2021, W214 222 6349-1/12E) als auch den Obersten Gerichtshof (OGH 18. Februar 2021, 6 Ob 127/20z) in mehrfacher Weise bestätigt.

Vor diesem Hintergrund stellte die in der Österreichischen Datenschutzbehörde eigens dafür eingerichtete Post-Task-Force im Jahr 2021 in knapp 50 Individualbeschwerdefällen abermals die rechtswidrige Verarbeitung der „Parteiaffinität“ durch die Österreichische Post fest. Im Sinne dieser Rechtsprechung wurde überdies in rund 60 Fällen eine Verletzung im Recht auf Geheimhaltung aufgrund der Verarbeitung der „Sinus-Geo-Milieus“ - welche (gleichermaßen vermutete) weltanschauliche Überzeugungen wiedergeben - ausgesprochen. Der erfolgreiche Abschluss von rund 135 Verfahren im Berichtszeitraum bei gleichzeitig signifikantem Rückgang der Ersteingaben führte schließlich zur Beendigung der Arbeit der Post-Task-Force mit Ende des Jahres 2021.

Die weiterhin bei der Datenschutzbehörde anhängigen Beschwerdeverfahren wegen mangelhafter Auskunftserteilung, deren Hauptgegenstand die Frage der Benennung konkreter Empfänger ist, wurden hingegen aufgrund eines entsprechenden Vorabentscheidungsersuchens des Obersten Gerichtshofes vom 18. Februar 2021 bis zur verbindlichen Normauslegung durch den Europäischen Gerichtshof im Verfahren C-154/21 größtenteils ausgesetzt. Gleichermaßen ausgesetzt wurden Verfahren im Zusammenhang mit der Frage, ob es sich bei Zuordnung des Datensatzes „Ehepaar traditionell“ um eine Verarbeitung sensibler Daten im Sinne von Art. 9 DSGVO handelt (EuGH C-252/21).

Weitere wesentliche Entscheidungen:

- 1. Bescheid vom 16. August 2021, GZ: 2021-0.432.224, rechtskräftig; Bescheid vom 25. August 2021, GZ: 2021-0.263.076, und Bescheid vom 14. Oktober 2021, GZ: 2021-0.277.070, beide nicht rechtskräftig (Weiterverarbeitung zu Marketingzwecken von im Rahmen eines Nachsendeauftrags bzw. der Einrichtung eines Urlaubspostfaches erhobenen Daten)**

In den oben genannten, im Wesentlichen gleichgelagerten Fällen hatte sich die DSB mit der Frage auseinanderzusetzen, ob die im Rahmen der Einrichtung eines Nachsendeauftrages bzw. Urlaubspostfaches erhobenen Daten zu Marketingzwecken weiterverarbeitet werden dürfen. Im Ergebnis wurden die Beschwerden wegen Verletzung im Recht auf Geheimhaltung allesamt abgewiesen und die Zulässigkeit somit dem Grunde nach bejaht.

Als Universaldienstbetreiberin nach dem Postmarktgesetz bietet die Österreichische Post ihren Kundinnen und Kunden im Falle eines Umzugs die Möglichkeit der Einrichtung eines Nachsendeauftrags bzw. im Falle einer urlaubsbedingten Abwesenheit jene eines Urlaubspostfaches an. Diese so erhobenen Daten werden anschließend für Werbezwecke an Dritte übermittelt. Durch das Anklicken einer „Checkbox“ können betroffene Personen einer Datenweitergabe widersprechen.

Die DSB führte begründend aus, dass - abgeleitet aus der gesetzlichen Verankerung in § 151 GewO - in bestimmten Fallkategorien ein die Betroffeneninteressen überwiegendes und einwilligungsunabhängiges berechtigtes Interesse der Gewerbetreibenden vorliegen kann und in den genannten Fällen - sofern Daten weitergegeben worden sind - auch tatsächlich vorgelegen ist.

Die Bescheide vom 25. August 2021 und vom 14. Oktober 2021 sind nicht rechtskräftig, der Bescheid vom 16. August 2021 ist rechtskräftig.

2. Bescheid vom 16. November 2021, GZ: 2021-0.734.848 (Zweifel an Identität befreien nicht von Verpflichtung zur Reaktion auf ein Auskunftsbegehren)

Trotz des Vorliegens eines entsprechenden Antrags der betroffenen Person hatte es die Österreichische Post im vorliegenden Fall gänzlich unterlassen, antragsgemäße Maßnahmen zu setzen oder auf das Ersuchen in sonstiger Form zu reagieren. Erst infolge der Erhebung einer Beschwerde bei der Datenschutzbehörde teilte die Post mit, dass die begehrte Auskunft aufgrund von Zweifeln an der Identität der Beschwerdeführerin nicht erteilt werden könne.

Wenngleich im Laufe des Verfahrens die Zweifel an der Identität nachvollziehbar dargelegt worden sind, befreit die Nichterbringung des Identitätsnachweises nach Ansicht der DSB Verantwortliche nicht von ihrer Pflicht auf ein Auskunftsbegehren fristgemäß zu reagieren. Dementsprechend wurde der Beschwerde aufgrund der Verletzung im Recht auf Auskunft vollumfänglich stattgegeben.

Dieser Bescheid ist rechtskräftig.

3. Bescheid vom 27. September 2021, GZ: 2021-0.668.377 (Lebensphase „Single“ und Mindestjahreseinkommen sind im Unterschied zu Sinus-Geo-Milieus keine sensiblen Daten)

Mit vorliegender Entscheidung bekräftigte die DSB einmal mehr ihre Rechtsauffassung, dass es sich bei zugeordneten Informationen wie etwa „Konservativ“ oder „Bürgerliche Mitte“ (sog. „Sinus-Geo-Milieus“) um – wenn auch nur unterstellte - weltanschauliche Überzeugungen handelt, die mangels Erlaubnistatbestand nach Art. 9 Abs. 2 DSGVO rechtswidrig durch die Österreichische Post verarbeitet wurden.

Demgegenüber hielt die DSB jedoch auch fest, dass Informationen über ein vermutetes Mindestjahreseinkommen oder die mögliche Lebensphase des Beschwerdeführers (verfahrensgegenständlich „optimieren, Single, Alter 35 – 45 Jahre“) mangels Ableitbarkeit eines in Art. 9 Abs. 1 DSGVO abschließend aufgezählten Merkmales (wie etwa die sexuelle Orientierung) einer Interessensabwägung zugänglich sind, welche im vorliegenden Fall zugunsten der Post ausfiel. Die Beschwerde wegen Verletzung im Recht auf Geheimhaltung wurde daher in diesem Punkt abgewiesen.

Dieser Bescheid ist nicht rechtskräftig.

4. Bescheid vom 29. September 2021, GZ: 2021-0.568.642 (Unbedenklichkeitserklärung gemäß § 151 GewO)

Die beiden Beschwerdeführer nahmen die erteilte Auskunft eines Adressverlages und Direktmarketingunternehmens (Beschwerdegegner) zum Anlass, eine Beschwerde bei der Datenschutzbehörde einzubringen. Beschwerdegegenständlich war die Frage, ob die Beschwerdeführer dadurch in ihrem Recht auf Geheimhaltung verletzt worden waren, indem der Beschwerdegegner ihre Adressdaten, konkret Anrede, Name, Geburtsdatum und Anschrift, aus

den Kunden- und Interessentendateisystemen von zwei anderen Adress- und Direktmarketingunternehmen ermittelt hatte.

Die Datenschutzbehörde führte zunächst aus, dass § 151 GewO als „Sonderdatenschutzrecht“ Regelungen enthält, unter welchen Voraussetzungen Adressverlage und Direktmarketingunternehmen personenbezogene Daten ermitteln und verwenden dürfen. Der Beschwerdegegner legte im Verfahren Unbedenklichkeitserklärungen der beiden Adress- und Direktmarketingunternehmen vor, von denen er die Daten der Beschwerdeführer erhalten hatte. Darin bestätigten die beiden Adress- und Direktmarketingunternehmen, dass die Beschwerdeführer in geeigneter Weise über die Möglichkeit informiert worden waren, die Übermittlung ihrer Daten für Marketingzwecke Dritter zu untersagen, und dass die Beschwerdeführer keine entsprechende Untersagung vorgenommen hatten. Vor diesem Hintergrund erwies sich die Verarbeitung der Adressdaten Anrede, Name, Geburtsdatum sowie Anschrift der Beschwerdeführer gemäß § 151 Abs. 5 erster Satz GewO als zulässig und erwiesen sich die Beschwerden daher im Ergebnis als unbegründet

Dieser Bescheid ist rechtskräftig.

3.2.1.2 Grenzüberschreitende Fälle der DSB⁵

Im Jahr 2021 wurden bei der DSB 401 Beschwerdefälle eingebracht, die einen grenzüberschreitenden Sachverhalt iSd Art. 4 Z 23 DSGVO aufwiesen. In 407 Fällen wurde die DSB als betroffene Aufsichtsbehörde in das Verfahren einbezogen.

Die DSB war seit 25. Mai 2018 bis Ende 2021 in 57 Verfahren als federführende Aufsichtsbehörde gegenüber einem Verantwortlichen tätig, wobei den anderen betroffenen Aufsichtsbehörden iSd Art. 4 Z 22 DSGVO seitens der DSB im Jahr 2021 in 7 Verfahren ein Beschlussentwurf gemäß Art. 60 Abs. 3 DSGVO vorgelegt wurde.

Eines dieser Verfahren betraf Verletzungen im Recht auf Information gemäß Art. 13 f. DSGVO sowie im Recht auf rechtmäßige Datenverarbeitung gemäß Art. 6 DSGVO, in welchem die Datenschutzbehörde im Ergebnis keine Verletzung feststellen konnte. Zwei weitere Verfahren betrafen Verletzungen im Recht auf Auskunft gemäß Art. 15 DSGVO bzw. Löschung gemäß Art. 17 DSGVO, die im laufenden Verfahren beseitigt wurden. Zwei Verfahren wurden, nachdem die Datenschutzbehörde den Gegenstand der Beschwerde in angemessenem Umfang untersucht hatte, gemäß Art. 57 Abs. 1 lit. f DSGVO abgewiesen. Ein Verfahren betraf eine Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO, ein weiteres die Einstellung eines amtswegigen Prüfverfahrens.

Im Rahmen der grenzüberschreitenden Zusammenarbeit innerhalb und außerhalb eines konkreten Verfahrens machte die DSB im Jahr 2021 118 Mal von der gegenseitigen Amtshilfe iSd Art. 61 DSGVO Gebrauch und wurde selbst in 228 Fällen von anderen Aufsichtsbehörden kontaktiert.

Insgesamt wurden seit dem 25. Mai 2018 bis Ende 2021 von allen Aufsichtsbehörden 282 Beschlussentwürfe iSd Art. 60 Abs. 3 DSGVO vorgelegt, die in 521⁶ finale Beschlüsse iSd Art. 60 Abs. 6 DSGVO mündeten.

Gegen den Beschlussentwurf der irischen Datenschutzbehörde, im Rahmen eines amtswegigen Prüfverfahrens wegen der Transparenzverpflichtungen der Verbraucherdienste von WhatsApp Irland ge-

5 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.

6 Hiervon umfasst sind auch finale Beschlüsse betreffend grenzüberschreitende Verfahren, die durch gütliche Einigung beendet wurden und bei denen es zu keinem Beschlussentwurf kam.

genüber Nutzern und Nicht-Nutzern nach den Art. 12-14 DSGVO, 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 zu einer Einleitung des Streitbeilegungsverfahrens iSv Art. 65 Abs. 1 lit. a DSGVO kam.

Der Europäische Datenschutzausschuss überprüfte im Rahmen des Streitbeilegungsverfahrens zunächst, welche Einsprüche iSd 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.

Der Europäische Datenschutzausschuss sprach in seiner zweiten Entscheidung⁷ gemäß Art. 65 Abs. 1 lit. a DSGVO vom 28. Juli 2021 mit Zweidrittelmehrheit aus, dass die irische Aufsichtsbehörde in ihrer Entscheidung eine Verletzung des in Art. 5 Abs. 1 lit. a DSGVO verankerten Transparenzgrundsatzes sowie von Art. 13 Abs. 1 lit. d DSGVO aufzunehmen habe. Zudem hielt der Europäische Datenschutzausschuss fest, dass im sog. „Lassy Hashing Verfahren“ keine Anonymisierung der erhobenen Daten von Nicht-Nutzern aus der Kontaktliste der Nutzer erfolge und daher auch diesbezüglich eine Verletzung des Art. 14 DSGVO anzunehmen sei. Weiters wurde die Frist zur Umsetzung des irischen Beschlusses von sechs auf drei Monate herabgesetzt und die irische Aufsichtsbehörde angewiesen, iSd Art. 83 Abs. 1 DSGVO in Bezug auf die Strafbemessung zusätzlich zum schwerwiegendsten Verstoß auch die anderen festgestellten Verletzungen zu berücksichtigen. Bei der Bemessung der Strafhöhe hielt der Europäische Datenschutzausschuss überdies fest, dass die irische Aufsichtsbehörde den Gesamtumsatz aller Teilgesellschaften des Unternehmens und sohin den konsolidierten Umsatz der Muttergesellschaft (Facebook Inc.) zu berücksichtigen habe und dass im Beschluss der federführenden Aufsichtsbehörde das vorangegangene Geschäftsjahr zur Berechnung der Geldbuße heranzuziehen sei.

Mit Entscheidung vom 20. August 2021 setzte die irische Datenschutzbehörde die Entscheidung des Europäischen Datenschutzausschusses um⁸ und setzte eine Geldbuße von € 225.000.000,-- fest (siehe auch dazu Kapitel 6.1.1.).

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 sowie ausführliche Informationen über die Rechte der betroffenen Personen und die Zuständigkeit der Datenschutzbehörde. Überarbeitet wurden unter anderem die Fragen und Antworten zum Coronavirus (COVID-19).

Darüber hinaus ist die Datenschutzbehörde gemäß Art. 57 Abs. 1 lit. e DSGVO verpflichtet, auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund der Datenschutzgrundverordnung zur Verfügung zu stellen und beantwortet allgemeine Anfragen zum geltenden Datenschutzrecht schriftlich. Telefonische Rechtsauskünfte werden nicht erteilt.

7 Die Entscheidung des EDSA ist unter folgendem Link abrufbar: https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12021-dispute-arisen_en.

8 https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf.

Im Rahmen der Beantwortung von Anfragen nimmt die Datenschutzbehörde grundsätzlich keine Vorabprüfung hinsichtlich der Zulässigkeit einer bestimmten Datenverwendung, der Anwendung bzw. Auslegung rechtlicher Bestimmungen oder einer sonstigen inhaltlichen Anfrage vor, da jede Antwort ein entsprechendes, vom Gesetz vorgesehene Verfahren vor der Datenschutzbehörde, präjudizieren würde.

3.2.3 Genehmigungen im Internationalen Datenverkehr

Die DSGVO sieht weitgehend eine Genehmigungsfreiheit für den internationalen Datenverkehr an Empfänger außerhalb des EWR vor. Die Übermittlung personenbezogener Daten an Empfänger in Drittländern oder in internationalen Organisationen ist in Kapitel V DSGVO geregelt. Sofern für den jeweiligen Zielort der Datenübermittlung kein Angemessenheitsbeschluss⁹ der Europäischen Kommission besteht, sieht Art. 46 DSGVO unterschiedliche rechtliche Instrumente zur Sicherstellung eines angemessenen Datenschutzniveaus¹⁰ vor.

Grundsätzlich ist eine Genehmigung dieser Instrumente durch die zuständige Aufsichtsbehörde nur mehr in bestimmten Fällen gemäß Art. 46 Abs. 3 DSGVO vorgesehen.

Eine Ausnahme bilden die sog. „Verbindlichen internen Datenschutzvorschriften“ (Binding Corporate Rules – BCRs), welche von der zuständigen Aufsichtsbehörde unter Anwendung des Kohärenzverfahrens gemäß Art. 63 ff DSGVO genehmigt werden.¹¹ Hierbei ist eine enge Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss notwendig.¹² Die in 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 zwingend zur Stellungnahme vorgelegt werden.¹³ Wegen 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 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, wie etwa durch die (neuen und modularen) Standarddatenschutzklauseln der Europäischen Kommission,¹⁴ erreicht werden kann. Dies ist vor allem dann empfehlenswert, wenn die Anzahl der Gruppenmitglieder in Drittländern gering ist. BCRs sollten nur dann zum Einsatz kommen, wenn die Nutzung anderer geeigneter Garantien problematisch erscheint.¹⁵

9 Eine Übersicht der derzeit geltenden Angemessenheitsbeschlüsse ist abrufbar in englischer Sprache unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

10 Siehe im Detail das Urteil des EuGH vom 16. Juli 2020, C-311/18.

11 Detaillierte Erläuterungen zu den materiellen Voraussetzungen von BCRs sind den beiden Arbeitsdokumenten WP256/rev.01 und WP257/rev.01 der ehemaligen Artikel-29-Datenschutzgruppe, welche derzeit vom Europäischen Datenschutzausschuss überarbeitet werden, zu entnehmen.

12 Das Prozedere ist im Arbeitsdokument WP263 rev.01 der ehemaligen Artikel-29-Datenschutzgruppe beschrieben, abrufbar in englischer Sprache unter <https://ec.europa.eu/newsroom/article29/items/623056/en>.

13 Siehe Art. 64 Abs. 1 lit. f DSGVO.

14 Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, ABl. L 2021/199, S. 31.

15 Vgl. hierzu das Arbeitsdokument WP74 der ehemaligen Artikel-29-Datenschutzgruppe.

Als weitere Übermittlungsgrundlage kommen ferner Verhaltensregeln (Art. 40 DSGVO) und Zertifizierungen (Art. 42 DSGVO) in Betracht, sofern sie ausreichende Bestimmungen zur Sicherstellung eines angemessenen Datenschutzniveaus enthalten.¹⁶ Auch in diesen Fällen ist eine Befassung des Europäischen Datenschutzausschusses sowie der Europäischen Kommission vorgesehen.¹⁷

Bei der Datenschutzbehörde wurden im Jahr 2021 keine Genehmigungsverfahren nach Kapitel V DSGVO 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 2021

Die Datenschutzbehörde hat im Jahr 2021 27 Bescheide im Rahmen der §§ 7,8 DSG erlassen – davon acht Zurückweisungen. Gründe hierfür waren beispielsweise mangelnde Aktivlegitimation der Antragsteller, eine fehlende unterfertigte Erklärung bzw. ein diese Erklärung ersetzender Exekutionstitel gem. § 7 Abs. 3 DSG oder eine nicht genehmigungsbedürftige Datenverarbeitung, da gem. § 7 Abs. 1 Z 3 DSG die Daten für den Verantwortlichen pseudonymisiert waren und dieser die Identität der betroffenen Personen mit rechtlich zulässigen Mitteln nicht bestimmen konnte.

15 Entscheidungen betrafen gemäß § 7 DSG zu Forschungszwecken erteilte Genehmigungen. Die Genehmigung von Bilddatenverarbeitungen betreffend den Straßenverkehr wurde besonders häufig beantragt. Beispiele hierfür waren die Verarbeitung von Bilddaten an öffentlichen Orten zum Zweck der Erforschung von Sicherheitsrisiken im Fahrradverkehr sowie zur Bewertung der Qualität der Radfahrinfrastruktur, zur Entwicklung eines Radars für eine sicherere Fahrassistenz und autonome Fahrfunktionen sowie die Entwicklung einer Hard- und Software zur Objekterkennung mittels Deep-Learning-Algorithmen.

Besonders hervorzuheben ist ein abweisender Bescheid, der ein anderes Thema zu Grunde liegen hatte. Mit Bescheid vom 18. Mai 2021 zur VZ D202.273 (GZ 2021-0.353.457) wies die Datenschutzbehörde den Antrag, es möge für die Veröffentlichung von personenbezogenen Daten - konkret Adresse, Bezeichnung, Bauzeit, Architekt, Mitarbeiter (Statiker, Planer, Freiraumplaner etc.), Baubeschreibung, Bauherr (wenn öffentlich) – rund 3.000 Bauobjekte betreffend, die Genehmigung erteilt werden, ab. In einer geplanten Publikation des Antragstellers, es ging um die Erstellung eines historischen Architekturführers für ein Bundesland, sollten diese Daten, wissenschaftlich aufbereitet, veröffentlicht werden. Dem Antrag wurde deswegen nicht entsprochen, weil eine a priori „Genehmigung einer Veröffentlichung“ von Daten § 7 DSG in verfassungskonformer Interpretation nicht zugeschrieben werden kann. Die

16 Art. 40 Abs. 3 bzw. Art. 42 Abs. 2 DSGVO. Entsprechende Leitlinien des EDSA sind in Ausarbeitung.

17 Vgl. etwa Art. 40 Abs. 3 iVm. Abs. 9 DSGVO.

Verweigerung der Genehmigung käme nämlich einer Zensurmaßnahme gleich, was in Form der Vorzensur jedenfalls grundrechtswidrig wäre.

3.2.5 Amtswegige Prüfverfahren

Die DSB hat im Jahr 2021 274 amtswegige Verfahren eingeleitet; 180 amtswegige Verfahren wurden im Berichtszeitraum einer Enderledigung (Bescheid oder Einstellung) zugeführt.

Ausgewählte Entscheidungen:

1. Bescheid vom 8. Februar 2021, GZ: D213.1166, 2020-0.849.832

Mit diesem Bescheid untersagte die Datenschutzbehörde einem Wasserverband die Datenverarbeitung durch ein Modell eines intelligenten Wasserzählers bzw. durch gleichwertige Modelle.

Zunächst hielt die Datenschutzbehörde fest, dass es sich bei der Erfassung von Informationen durch einen intelligenten Wasserzähler um eine Verarbeitung personenbezogener Daten handelt.

Der Verantwortliche ist gemäß § 87 Abs. 1 WRG 1959 als Körperschaft öffentlichen Rechts eingerichtet und verwaltet seine eigenen Angelegenheiten selbständig. Bei dem Betrieb der Verbandsanlagen ist er in Erfüllung seiner satzungsmäßigen Aufgaben gemäß § 89 WRG 1959 im Rahmen der Hoheitsverwaltung tätig. Die Einrichtung als Körperschaft des öffentlichen Rechts bedingt, dass der Verantwortliche als „Behörde“ im Sinne des § 1 Abs. 2 DSG zu qualifizieren ist. Demnach darf die Verwendung personenbezogener Daten nur auf Basis einer ausreichend determinierten Rechtsgrundlage erfolgen.

Die Datenschutzbehörde kam gegenständlich zum Ergebnis, dass der Verantwortliche die Datenverarbeitung auf keine geeignete Rechtsgrundlage iSd § 1 Abs. 2 DSG iVm Art. 6 Abs. 1 lit. b und e DSGVO stützen konnte.

Der Bescheid ist nicht rechtskräftig.

2. Bescheid vom 29. Juli 2021, GZ: D213.1303, 2021-0.412.072

In diesem – aufgrund eines anonymen Hinweises eingeleiteten – Verfahren, kam die Datenschutzbehörde zu dem Ergebnis, dass die Verarbeitung personenbezogener Daten von 73 Personen zwischen Jänner und März 2021 für Zwecke interner Ermittlungen unrechtmäßig war.

Die Verantwortliche hat interne Ermittlungen eingeleitet, weil vertrauliche Informationen in Form eines Zeitungsartikels an die Öffentlichkeit gelangt sind. Die betroffenen Mitarbeiter wurden mit Schreiben samt Einwilligungserklärung über den Gegenstand sowie den Zeitraum der Untersuchung informiert. Im Rahmen der Ermittlungen wurden zum einen ihre E-Mail Konten nach Suchbegriffen untersucht, zum anderen wurde ein Abgleich der Telefonverbindungen mit bestimmten Zieltelefonnummern bei den Diensthandys der jeweiligen Mitarbeiter durchgeführt.

Der Betriebsrat wurde von diesen Untersuchungen nicht in Kenntnis gesetzt. Ebenso fehlte die Zustimmung desselben für die eingeleiteten Maßnahmen.

Die Datenschutzbehörde kam gegenständlich zum Ergebnis, dass keine gültigen Einwilligungserklärungen der betroffenen Personen eingeholt wurden, da die betroffenen Personen im Falle der Nichterteilung der Einwilligung in eine Drucksituation geraten würden. Außerdem man-

gelte es der Einwilligungserklärung auch an der erforderlichen Information darüber, welche Folgen die Nichterteilung der Einwilligung hat.

Auch auf berechnigte Interessen konnte die von der Verantwortlichen vorgenommene Datenverarbeitung nicht gestützt werden, da die durchgeführte interne Untersuchung eine zustimmungspflichtige Maßnahme nach § 96 Abs. 1 Z 3 ArbVG darstellte. Da keine Zustimmung des Betriebsrates vorlag und die Datenverarbeitung daher schon deshalb rechtswidrig wäre, konnte die vorgenommene Datenverarbeitung auch nicht auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden.

Dieser Bescheid ist nicht rechtskräftig.

3. Bescheid vom 9. August 2021, GZ: D213.1239, 2021-0.351.928

In diesem Fall ging es darum, dass der Leiter einer Tennisschule ein Foto, auf welchem er mit drei Kindern abgelichtet ist, auf einer Online-Dating-Plattform veröffentlicht hat. Die betroffenen Personen bzw. deren Erziehungsberechtigte wurden nicht informiert und haben auch nicht in die Veröffentlichung eingewilligt.

Der Verantwortliche hat zwar dazu kein konkretes Vorbringen erstattet, aus seinen Stellungnahmen gegenüber der Datenschutzbehörde ging jedoch hervor, dass er ein Interesse daran hatte, Fotos von Dritten, die an seinen Tennisveranstaltungen teilnehmen, zur Bewerbung seiner Dienstleistungen in seinen Medien zu verwenden.

Davon war im gegenständlichen Fall schon deshalb nicht auszugehen, da die Veröffentlichung auf einer Online-Dating-Plattform erfolgte, welche nicht darauf abzielt, eigene Dienstleistungen zu bewerben, sondern Partner für private Zwecke zu finden.

Schon aus diesem Grund lag kein berechtigtes Interesse des Verantwortlichen vor, das zu berücksichtigen gewesen wäre.

Die Veröffentlichung konnte damit nicht auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden und war daher entgegen des in Art. 5 Abs. 2 lit. a DSGVO normierten Rechtmäßigkeitsgrundsatzes erfolgt.

Die Datenschutzbehörde kam daher zu dem Ergebnis, dass die gegenständliche Datenverarbeitung unrechtmäßig erfolgt ist.

Dieser Bescheid ist rechtskräftig.

4. Bescheid vom 16. November 2021, GZ: D213.1093; 2021-0.023.416

Dieses Verfahren wurde eingeleitet, weil der Datenschutzbehörde ein USB-Stick von einem anonymen Absender übermittelt wurde. Wie sich herausstellte, stand dieser im Eigentum der Leiterin einer Justizanstalt. Ein Mitarbeiter der Justizanstalt hat Anfang Februar 2020 den USB-Stick widerrechtlich an sich genommen und die am USB-Stick gelöschten Dateien wiederhergestellt. Unter den mehr als 2000 wiederhergestellten Dateien haben sich u.a. Protokolle über Sitzungen des Dienstenausschusses, Protokolle über Befragungen der Mitarbeiter der Justizanstalt im Rahmen der Dienstaufsicht, in denen u.a. Angaben über Erkrankungen und den Gesundheitszustand der Mitarbeiter dokumentiert sind, befunden.

Eine Verschlüsselung der darauf befindlichen Dokumente wurde seitens der Verantwortlichen nicht vorgenommen und verfügte diese bis März 2020 auch über keine Kenntnisse über die technischen Voraussetzungen für die Verschlüsselung von Datenträgern.

Im Ergebnis konnte gegenständlich von keinen Art. 32 DSGVO bzw. § 54 Abs. 2 Z 2 DSG genügenden Maßnahmen ausgegangen werden und fiel dies der Verantwortlichen zur Last (siehe Art. 5 Abs. 2 DSGVO bzw. § 37 Abs. 3 DSG), weshalb die Datenschutzbehörde zum Ergebnis gelangte, dass es die Verantwortliche im Rahmen ihrer Funktion als Leiterin der Justizanstalt durch den Gebrauch eines privaten sowie ungesicherten Datenträgers, auf welchem sie dienstliche Dokumente verarbeitet hat, unterlassen hat, eine angemessene Sicherheit der Datenverarbeitung zu gewährleisten.

Dieser Bescheid ist nicht rechtskräftig.

3.2.6 Beschwerdeverfahren vor dem Bundesverwaltungsgericht einschließlich Säumnisbeschwerden

Im Jahr 2021 wurden 511 Beschwerden gegen Bescheide der Datenschutzbehörde erhoben.

Es gab 56 Säumnisbeschwerden im Berichtszeitraum.

W211 2222613- 2/11E und W211 2222613 -2/12E, Teilerkenntnis und Beschluss vom 9. August 2021

Die Datenschutzbehörde wies eine Beschwerde zur Geschäftszahl 2021-0.568.752 (D124.059) wegen Verstoßes gegen das Auskunftsrecht (insbesondere hinsichtlich Art. 15 Abs. 1 lit. d, g, und Abs. 3 DSGVO) und Verstoßes gegen Informationspflichten gemäß Art. 14 DSGVO ab (Spruchpunkte 1. und 2.), sowie wegen Verletzung im Recht auf Geheimhaltung aufgrund eines Verstoßes gegen die Datenminimierungspflicht sowie gegen die Datensicherungspflichten gemäß Art. 25 DSGVO zurück (Spruchpunkt 3.).

In Bezug auf Spruchpunkt 1. gab das Bundesverwaltungsgericht der Beschwerde teilweise statt und stellte fest, dass die mitbeteiligte Partei den Beschwerdeführer dadurch in seinem Recht auf Auskunft verletzt habe, dass sie eine unzureichende Auskunft im Sinne des Art. 15 Abs. 1 lit. d DSGVO hinsichtlich der geplanten Dauer, für die die personenbezogenen Daten gespeichert werden (bzw. die Kriterien für die Festlegung dieser Dauer) erteilt habe. In Bezug auf die Beschwerdepunkte betreffend die Erteilung der Auskunft über die Herkunft der Daten und die Verarbeitungszwecke wurde die Beschwerde abgewiesen.

Hinsichtlich Spruchpunkt 2. wurde der Beschwerde stattgegeben und festgestellt, dass die mitbeteiligte Partei gegen ihre Informationspflicht nach Art. 14 Abs. 1 lit. e DSGVO verstoßen habe. Das Bundesverwaltungsgericht begründete seine Entscheidung damit, dass die mitbeteiligte Partei gemäß Art. 14 Abs. 3 lit. c DSGVO spätestens zum Zeitpunkt der ersten Offenlegung über die Offenlegung an eine/n andere/n Empfänger zu informieren gehabt hätte.

Der 3. Spruchpunkt des Bescheids der Datenschutzbehörde wurde seitens des Bundesverwaltungsgerichts geteilt – im Hinblick auf das Recht auf Geheimhaltung gemäß § 1 DSG sei die Zurückweisung zu Recht, bezüglich der geltend gemachten Verstöße gegen die Datenminimierungspflicht nach Art. 5 DSGVO sowie die Datensicherungspflichten nach Art. 25 DSGVO zu Unrecht erfolgt. Letzteres begründete das Bundesverwaltungsgericht damit, dass entgegen der Annahme der Datenschutzbehörde keine unzulässige Änderung des Wesens der Datenschutzbeschwerde gemäß § 13 Abs. 8 AVG vorgelegen sei, da die mitbeteiligte Partei bereits in der Beschwerde dahingehende Ausführungen getätigt habe. Die Zurückweisung im Hinblick auf § 1 DSG sei hingegen zu Recht erfolgt, da die mitbeteiligte Partei hierzu keine inhaltlichen Ausführungen vorgebracht habe.

Das Teilerkenntnis ist nicht rechtskräftig, es wurde seitens der Datenschutzbehörde Amtsrevision erhoben.

Der Beschluss des Bundesverwaltungsgerichts vom 9. August 2021 betrifft die Aussetzung des Verfahrens und Vorlage gemäß Art. 267 AEUV an den Gerichtshof der Europäischen Union (EuGH). Für das Bundesverwaltungsgericht hätten sich Zweifel an der richtigen Auslegung bezüglich der Zurverfügungstellung einer Kopie der personenbezogenen Daten nach Art. 15 Abs. 3 DSGVO ergeben, weshalb diesbezüglich insgesamt vier Fragen vorgelegt wurden. Das Verfahren ist zur Zahl C-487/21 anhängig.

W245 2232826-1/36E Erkenntnis vom 11. Mai 2021

Mit diesem Erkenntnis bestätigte das Bundesverwaltungsgericht einen Bescheid der Datenschutzbehörde vom 20. Mai 2020, GZ: 2020-0. 256. 089 (DSB-D130. 357), mit dem eine Beschwerde, welche die Entfernung von Ergebnissen einer Suchmaschine zu einem abgeschlossenen Gerichtsverfahren des Beschwerdeführers zum Gegenstand hatte, abgewiesen wurde.

Der Beschwerdeführer begehrte ursprünglich eine Nichtaufnahme bestimmter Informationen in den Index des Suchmaschinenbetreibers, später jedoch nur mehr einen Suchfilter. Im Laufe des verwaltungsrechtlichen Verfahrens stellte sich heraus, dass die vom Beschwerdeführer monierten Einträge in der Ergebnisliste der Suchmaschine nicht mehr enthalten waren.

Das Bundesverwaltungsgericht führte zur Abweisung der Bescheidbeschwerde zusammengefasst aus, dass die vom Beschwerdeführer beantragte Maßnahme – nämlich die Löschung/Unterdrückung von Suchergebnissen in der Suchmaschine ohne Validierung der Quellseiten – weder geeignet noch verhältnismäßig sei. Die Eignung scheitere bereits daran, dass die begehrte Maßnahme lediglich bei Eingabe von Vor- und Nachname funktioniere, bei Eingabe etwa lediglich des Nachnamens plus eines passenden anderen Begriffs jedoch fehlschlage. Zusätzlich sei der Beschwerdeführer nicht die einzige Person mit diesem Namen und eine Unterdrückung von Suchergebnissen pro futuro könnte auch Ergebnisse treffen, die nichts mit dem ursprünglichen Thema der Unterlassungsforderungen zu tun haben. Eine Handlungspflicht für den Betreiber der Suchmaschine könne erst durch einen konkreten Hinweis (eine konkrete URL) begründet werden, weil er erst dadurch Kenntnis von einer offensichtlich und auf den ersten Blick klar erkennbaren Rechtsverletzung erlangt.

Es sei unzulässig, Suchergebnisse nur deshalb zu löschen bzw. zu unterdrücken, weil eine URL bestimmte Suchwörter enthält. Vielmehr müsse jeweils die dahinterliegende Quellseite überprüft und einer Interessenabwägung unterzogen werden.

Das Bundesverwaltungsgericht ließ die Revision gleich aus mehreren Gründen zu. Es fehle an Rechtsprechung des Verwaltungsgerichtshofs zur Frage, ob aus der DSGVO bzw. dem DSG ein eigenständiger Feststellungsanspruch über Rechtsverletzungen in der Vergangenheit zu entnehmen ist, ob eine Antragsänderung - zunächst Unterlassung der Indexierung, später keine Einschränkung einer Indexierung, jedoch Eingrenzung einer Auswertung von Informationen aus dem Index durch vordefinierte Suchbegriffe - die subjektiven Rechte des Verpflichteten weniger einschränken und daher diese Änderung bloß zu einem „MINUS“ und nicht zu einem „ALIUD“ gemäß § 66 Abs. 4 AVG führt und ob aus der DSGVO ein Anspruch auf vorbeugenden Rechtsschutz abgeleitet werden kann, womit die betroffene Person dauerhaft einen Anspruch auf Löschung der relevanten Inhalte hätte.

Das Erkenntnis ist nicht rechtskräftig, da der Beschwerdeführer Revision erhoben hat.

W211 2227667-1/5E, Erkenntnis vom 30. Juli 2021

Das Bundesverwaltungsgericht hat mit diesem Erkenntnis die Beschwerde gegen den Bescheid der DSB vom 19. November 2019, GZ: DSB-D124. 857/0006- DSB/2019, wegen einer Verlet-

zung im Recht auf Geheimhaltung unter Maßgabe der Abänderung des Spruchpunkts 1. als unbegründet abgewiesen.

Im bekämpften Bescheid hatte die Datenschutzbehörde der Beschwerde wegen einer Verletzung im Recht auf Geheimhaltung durch die Weiterleitung einer E-Mail an andere Miteigentümer eines Wohnhauses durch eine Hausverwaltung teilweise stattgegeben.

Das Bundesverwaltungsgericht hielt die teilweise Stattgabe der Datenschutzbehörde im Ergebnis zwar aufrecht, stellte allerdings nunmehr ausschließlich die Unrechtmäßigkeit der Verarbeitung in Ermangelung eines berechtigten Interesses gem. Art. 6 Abs. 1 lit. f DSGVO bzw. eines sonstigen Erlaubnistatbestandes des Art. 6 Abs. 1 DSGVO fest. Eine Verletzung im Recht auf Geheimhaltung wurde jedoch ausdrücklich verneint.

Das Bundesverwaltungsgericht führte dazu begründend aus, dass § 20 WEG zwar grundsätzlich ein berechtigtes Interesse von Hausverwaltungen gemäß Art. 6 Abs. 1 lit. f DSGVO begründen könne, ein solches im gegenständlichen Fall jedoch nicht gegeben sei, da die Offenlegung der Korrespondenz durch die nunmehrige Beschwerdeführerin nicht zur Erfüllung ihrer Aufgaben nach dem WEG erforderlich gewesen sei. Eine Verletzung im Recht auf Geheimhaltung wurde jedoch mit der Begründung verneint, dass der Mitbeteiligte (und vormalige Beschwerdeführer) seinen Namen, seine Postleitzahl sowie seine E-Mail-Adresse als Impressum auf seiner Website publiziert und sich dort gerade mit Fragen der Eigentümergemeinschaft und Verwaltung der fraglichen Liegenschaft auseinandergesetzt habe, weshalb kein schutzwürdiges Geheimhaltungsinteresse gegenüber anderen Miteigentümern bestehen würde. Auch hinsichtlich der Offenlegung von Abstimmungsunterlagen gegenüber anderen Miteigentümern lasse sich ein solches Interesse nicht erkennen.

Dieses Erkenntnis ist nicht rechtskräftig, die Hausverwaltung hat Revision erhoben.

W256 2227693-1/10E, Erkenntnis vom 31. August 2021

Die Datenschutzbehörde leitete ein amtswegiges Prüfverfahren (Art. 58 Abs. 2 lit. b DSGVO iVm § 22 DSG) zur Prüfung der „Einhaltung der Bestimmungen der DSGVO und des DSG“ gegen den Betreiber eines Kundenbindungsprogrammes ein, bei dem insbesondere die Datenverarbeitungen zum Zweck des Profiling im Zusammenhang mit dem Bindungsprogramm überprüft wurden.

Mit Beschwerdevorentscheidung vom 11. Dezember 2019, GZ: DSB-D062.297/0001-DSB/2019, wurde festgestellt, dass die für diese Datenverarbeitung eingeholten Einwilligungen nicht den Anforderungen der Art. 4 Z 11 DSGVO und Art. 7 DSGVO entsprechen und die Datenverarbeitung daher mangels Rechtsgrundlage unzulässig sei. Zusätzlich wurde die Datenverarbeitung von der Datenschutzbehörde untersagt.

Mit Erkenntnis des Bundesverwaltungsgerichts wurde der Beschwerde des Verantwortlichen stattgegeben und der Bescheid ersatzlos behoben. Das Bundesverwaltungsgericht hielt dazu begründend fest, dass sich die Datenschutzbehörde lediglich mit der Rechtsgrundlage der Einwilligung auseinandergesetzt habe und daher die Prüfung anderer Rechtsgrundlagen nicht vom Prüfgegenstand umfasst gewesen sei. Die bloße Auseinandersetzung mit der Rechtsgrundlage der Einwilligung könne aber nicht ohne weiteres einen Verstoß gegen den „Grundsatz der Rechtmäßigkeit“ und damit auch keine darauf gestützte Berechtigung zur Ausübung einer Abhilfebefugnis nach Art. 58 Abs. 2 lit. d und f DSGVO begründen.

Bereits aus dem Wortlaut des Art. 6 Abs. 1 DSGVO („[.] wenn mindestens [.]“) gehe deutlich hervor, dass eine Datenverarbeitung nicht nur auf einen, sondern eben auf mehrere, gleichrangig nebeneinanderstehende Rechtsgrundlagen gestützt werden könne. Auch sei es im Falle einer ungültigen Einwilligung nicht generell unmöglich, auf andere Rechtsgrundlagen – wie etwa Art. 6 Abs. 1 lit. f DSGVO – zurückzugreifen. Das Bundesverwaltungsgericht kommt dabei zum Schluss, dass der „Grundsatz der Rechtmäßigkeit“ von den „Grundsätzen der Transparenz und der Verarbeitung nach Treu und Glauben“ unabhängig zu betrachten ist.

Das Erkenntnis ist nicht rechtskräftig, es wurde seitens der Datenschutzbehörde Amtsrevision erhoben.

W214 2226349-1/12E und W214 2226350-1/17E, Erkenntnis vom 20. Mai 2021

Im Bescheid vom 6. September 2019, DSB-D205.179.000/1-DSB/2019, wurde einer Beschwerde im Zusammenhang mit der Verarbeitung von „Parteiaffinitäten“ (vgl. zu diesem Themenkomplex Punkt 3.2.1.1.) teilweise stattgegeben und festgestellt, dass die Beschwerdeführerin durch die Verarbeitung ihrer Daten betreffend „Parteiaffinität“ in ihrem Recht auf Geheimhaltung verletzt wurde und diese Daten zu löschen seien. Die begehrte Feststellung, nach der § 151 GewO rechtswidrig, unionsrechtswidrig und unverhältnismäßig sei, wurde zurückgewiesen. Jenes Feststellungsbegehren, nach der eine Verletzung der Informationspflichten erfolgt sei, wurde wiederum abgewiesen.

Das Bundesverwaltungsgericht bestätigte im gegenständlichen Erkenntnis zunächst die Ansicht der Datenschutzbehörde, nach welcher auch statistisch errechnete „Parteiaffinitäten“ als personenbezogene Daten zu werten sind (und dabei als „Daten besonderer Kategorie“ gemäß Art. 9 DSGVO), wenn sie betroffenen Personen zugeordnet werden (siehe hierzu das Teilerkenntnis des Bundesverwaltungsgerichts vom 20. August 2020, W 258 2217446-1 und mittlerweile auch das Erkenntnis des Verwaltungsgerichtshofs vom 14. Dezember 2021, Ro 2021/04/0007 -4). § 151 GewO stelle dabei aufgrund eines mangelnden erheblichen öffentlichen Interesses keine ausreichende Rechtsgrundlage iSd. Art. 9 Abs. 2 lit. g DSGVO dar. Das Bundesverwaltungsgericht hielt hierzu weiters fest, dass der Datenschutzbehörde eine Feststellungskompetenz hinsichtlich des Verstoßes gegen das Recht auf Geheimhaltung zukomme.

Da das Bundesverwaltungsgericht die Rechts- und Sachlage zum Zeitpunkt der Entscheidung im verwaltungsbehördlichen Verfahren zu berücksichtigen hat, war der erteilte Löschauftrag hingegen zu beheben, da die Daten bereits gelöscht waren und der Auftrag dazu daher obsolet war.

Das Bundesverwaltungsgericht bestätigte außerdem die Spruchpraxis der DSB, nach der auch Beschwerden wegen Verstoßes gegen die Informationspflichten gemäß Art. 13 und 14 DSGVO einer nachträglichen Heilung iSd. § 24 Abs. 6 DSG zugänglich sind. Da Art. 77 Abs. 1 DSGVO kein zwingendes Recht auf die Feststellung vergangener Rechtsverletzungen vorschreibe, könne in § 24 Abs. 6 DSG auch keine Unionsrechtswidrigkeit erblickt werden.

Die Zurückweisung des Antrags auf Feststellung der Unionsrechtswidrigkeit von § 151 GewO sei ebenfalls nicht zu beanstanden, da die Datenschutzbehörde die Beurteilung der Gesetzmäßigkeit der Norm nicht aufzugreifen habe (vgl. VwGH 18.5.1988, 88/92/0050), sie gemäß Art. 89 B -VG keine Normenkontrollinstanz sei und zudem die Formulierung einer Vorlagefrage gemäß Art. 267 AEUV mangels Tribunaleigenschaft unzulässig sei.

Dieses Erkenntnis ist nicht rechtskräftig, es wurde mittels ordentlicher Revision bekämpft.

W256 2235360-1/5E, Erkenntnis vom 1. Dezember 2021

Die Datenschutzbehörde hat mit Bescheid vom 28.02.2020, GZ: DSB-D123.685/0009-DSB/2019, ausgesprochen, dass eine Verletzung im Recht auf Geheimhaltung vorliegt, wenn Amtshandlungen der Polizei veröffentlicht werden, welche die PolizistInnen etwa mit Hasenohren oder begleitet von anzüglichen Emojis zeigen. Bezüglich sonstiger Aufnahmen wurde die Beschwerde abgewiesen.

Das Bundesverwaltungsgericht gab der Bescheidbeschwerde der Betroffenen statt und hielt fest, dass gegenständlich auch eine Verletzung im Recht auf Geheimhaltung vorliegt, wenn Bild- und Videoaufnahmen von Polizeipersonal auf Instagram oder Facebook veröffentlicht werden, die diese identifizierbar bei einer Amtshandlung zeigen. Es führte hierzu begründend zunächst aus, dass es zwar zulässig sei, Handlungen der Polizei aufzuzeigen, ein „Vorführen“ oder „Heruntermachen“ vor der breiten Öffentlichkeit sei jedoch nicht zulässig. Gegenständlich sei aber außerdem eindeutig nicht das gelindeste, zum Ziel führende Mittel gewählt worden. So seien etwa die Gesichter der Betroffenen nicht unkenntlich gemacht worden, obwohl die Offenlegung der jeweiligen Identitäten nicht für den angestrebten Zweck notwendig gewesen sei. Das Bundesverwaltungsgericht hielt hierzu u.a. auch fest, dass diese Veröffentlichungen mit Kommentaren gegen die PolizistInnen einhergingen, die unbewiesene bzw. falsche Vorwürfe enthielten. Demgegenüber konnte der Beschwerdeführer keine Gründe nennen, welche die Interessenabwägung zugunsten einer Veröffentlichung ausschlagen lassen würden (zB Informationsbedürfnis der Öffentlichkeit).

Dieses Erkenntnis ist rechtskräftig

3.2.6a Beschwerdeverfahren vor dem Bundesverwaltungsgericht in Verwaltungsstrafsachen

Beschuldigte haben das Recht, gegen Straferkenntnisse und Verwarnungen bzw. Bescheide der Datenschutzbehörde eine Beschwerde zu erheben. Eine rechtzeitig eingebrachte (innerhalb von vier Wochen nach Zustellung) und zulässige Beschwerde hat aufschiebende Wirkung (der Bescheid bzw. die Geldbuße kann somit bis zur abschließenden Entscheidung nicht vollstreckt werden). Das Bundesverwaltungsgericht ist für die Beschwerden gegen Bescheide der Datenschutzbehörde zuständig.

Im Berichtszeitraum wurden 11 Beschwerden gegen Straferkenntnisse der Datenschutzbehörde erhoben.

Erkenntnis des Bundesverwaltungsgerichts vom 29.01.2021, GZ: W211 2232168-1

Das Bundesverwaltungsgericht hat mit gegenständlichem Erkenntnis einer Beschwerde teilweise Folge gegeben und die Strafe reduziert, jedoch wurde die Beschwerde ansonsten als unbegründet abgewiesen und das Straferkenntnis der Datenschutzbehörde dem Grunde nach bestätigt.

Im gegenständlichen Fall hat der Beschuldigte (Polizist) zum Zwecke privater Informationsinteressen auf das PAD-System (Aktenverwaltungssystem der Landespolizeidirektion) - ohne Berechtigung - zugegriffen und Einsicht in ein gegen seine Tochter geführtes Verfahren genommen. Der Beschuldigte war zwar generell dazu berechtigt, das PAD-System im Rahmen seiner dienstlichen Aufgaben als Exekutivbeamter zu verwenden, jedoch war er nicht der zuständige Sachbearbeiter des konkreten Aktes. Der Beschuldigte hat keine Änderungen im Akt vorgenommen, sondern nur den Inhalt gesichtet.

Das Bundesverwaltungsgericht führte im Rahmen der rechtlichen Beurteilung ins Treffen, dass die gegenständliche Verarbeitung bzw. Einsicht in den jeweiligen Akt nicht auf die Einwilligung der eigenen Tochter gestützt werden kann, da auch weitere Betroffene im Akt angeführt waren, insbesondere die Beamten der jeweiligen Polizeiinspektion, die die Ermittlungen gegen seine Tochter geführt haben sowie allfällige Zeugen und administrative Sachbearbeiter des Aktes.

Art. 6 Abs. 1 lit. c und e DSGVO kommt ebenfalls nicht in Betracht, da die Akteneinsicht ein antragspflichtiges Beschuldigtenrecht ist und nur vom jeweils zuständigen SB vorgenommen werden darf. Auch überwiegende berechnigte Interessen nach Art. 6 Abs. 1 lit. f DSGVO liegen im konkreten Fall nicht vor, da die Einsicht in den Akt jedenfalls nicht erforderlich war, um die Interessen des Beschuldigten zu wahren. Der Beschuldigte hätte als gesetzlicher Vertreter seiner Tochter einen Antrag auf Akteneinsicht stellen können. Der hierfür zuständige Sachbearbeiter hätte dann in Folge die Akteneinsicht gewährt. Ein Antrag auf Akteneinsicht stellt daher jedenfalls ein gelinderes Mittel dar und es wäre dem Beschuldigten auch zumutbar gewesen.

Darüber hinaus führte das BVwG aus, dass der Grundsatz der Zweckbindung verletzt wurde, da kein legitimer Zweck vorlag. Die Verarbeitung muss über das Erfordernis eines Rechtsgrundes im Sinne von Art. 6 Abs. 1 DSGVO hinaus auch im Einklang mit der Rechtsordnung stehen. Die gegenständliche Einsichtnahme war weder durch sachliche Zuständigkeit noch durch strafprozessuale Rechte gedeckt.

Der Beschuldigte wurde in diesem Zusammenhang als eigenständiger Verantwortlicher im Sinne des Art. 4 Z 7 DSGVO qualifiziert, da er in Bezug auf die Verarbeitung über Zwecke und Mittel entschieden hat. Sofern natürliche Personen für ihre eigenen Zwecke außerhalb des Tätigkeitsbereichs und der möglichen Kontrolle ihrer Organisation Daten verarbeiten, können sie selbst (nur in diesem Rahmen) Verantwortliche sein.¹⁸

Die Revision wurde zwar für zulässig erklärt, das Erkenntnis ist aber rechtskräftig.¹⁹

Erkenntnis des Bundesverwaltungsgerichts vom 02.06.2021, GZ: W211 2232587-1

Das Bundesverwaltungsgericht hat die Beschwerde des Beschwerdeführers als unbegründet abgewiesen und das bekämpfte Straferkenntnis der Datenschutzbehörde zur Gänze bestätigt. Der Beschwerdeführer wurde darüber hinaus zur Leistung von Verfahrenskosten in Höhe von 20% der verhängten Strafe als Beitrag zu den Kosten des Beschwerdeverfahrens verpflichtet (zusätzlich zu den Kosten des verwaltungsbehördlichen Verfahrens in Höhe von 10% der verhängten Strafe).

Im konkreten Fall betrieb der Beschuldigte als Verantwortlicher eine Videoüberwachungsanlage, bestehend aus mehreren Kameras, die vor und in einem Wettlokal installiert wurden. Es wurden insgesamt acht Kameras betrieben und waren mit einem Computer im Büro des Lokals verbunden. Zwei Kameras erfassten einen unmittelbar an das Lokal angrenzenden Gehsteig sowie einen öffentlichen Parkplatz. Die Aufzeichnungen der Anlage wurden 18 Tage lang aufbewahrt. Anhand der Aufzeichnungen erstellte der Beschuldigte „Screenshots“ und hängte diese im Büro des Lokales auf, um damit Spieler des Wettlokals von Beamten der Finanzpolizei zu unterscheiden bzw. diese Personen zu identifizieren. Die Videoüberwachungsanlage war darüber hinaus nicht gekennzeichnet.

¹⁸ Vgl. Hödl in Knyrim, DatKomm Art. 4 DSGVO, RZ 86.

¹⁹ Das Bundesverwaltungsgericht hat mit Erkenntnis vom 22.11.2021 darüber hinaus auch ein weiteres Straferkenntnis der Datenschutzbehörde wegen unrechtmäßigem Zugriff auf das PAD-System durch eine Beamtin dem Grunde nach bestätigt, da keine Berechnigung vorlag und nicht das gelindeste Mittel gewählt wurde, GZ: W214 2238581-1.

Das Bundesverwaltungsgericht führte im Rahmen der rechtlichen Beurteilung aus, dass keine überwiegenden berechtigten Interessen des Beschuldigten im Sinne des Art. 6 Abs. 1 lit. f DSGVO vorliegen, da die Interessenabwägung zu Gunsten der Betroffenen ausfällt (das grundrechtlich geschützte Recht auf Geheimhaltung der in den Aufnahmebereich der Anlage gelangenden Verkehrsteilnehmer überwiegt ein allfälliges Interesse am Betrieb der Anlage). Außerdem stellte der Zweck der Anlage (Identifizierung und Kategorisierung von Spielern und Beamten) keinen legitimen Zweck dar, da dadurch auch gegen andere Vorgaben der Rechtsordnung verstoßen wurde, wie jene der Durchführung von Glücksspiel im gesetzlich vorgegebenen Rahmen.

Schließlich führte das Bundesverwaltungsgericht zur konkreten Speicherdauer aus, dass diese auf das unbedingt erforderliche Mindestmaß für die Erreichung des Zwecks zu beschränkt ist (Einzelfallbeurteilung). Auf Grund der konkret gewählten Speicherdauer (18 Tage) verstieß der Beschuldigte auch gegen den Grundsatz der Speicherbegrenzung. Es lagen im Rahmen des Verfahrens keinerlei Hinweise vor, dass mit der Speicherung der Daten für eine derart lange Zeit tatsächlich ein unbedingt erforderliches Mindestmaß eingehalten wurde. Selbst zum Zwecke der Objektüberwachung wäre eine derart lange Speicherdauer nicht erforderlich. Abschließend führte das Bundesverwaltungsgericht in Bezug auf die Bestimmtheit der Strafbestimmungen der DSGVO aus, dass Art. 5 Abs. 1 lit. e DSGVO das Erfordernis der ausreichenden Bestimmtheit erfüllt. Es wird zwar anerkannt, dass dieser Grundsatz keine erlaubte Höchstdauer (z.B. früher 72 Stunden) beinhaltet, jedoch geht aus dieser Bestimmung ausreichend klar hervor, dass die Speicherdauer auf ein Mindestmaß und in einem direkten Bezug auf die Zweckbindung beschränkt ist. Der Beschuldigte nahm im vorliegenden Fall jedoch keine nachvollziehbaren Überlegungen zur Speicherdauer vor.

Auch der Verstoß wegen mangelnder Kennzeichnung der Kamera (Art. 5 Abs. 1 lit. a iVm Art. 12 und 13 iVm Art. 83 Abs. 1 und Abs. 5 lit. a DSGVO) wurde vom Bundesverwaltungsgericht bestätigt, da der Beschuldigte keine Kennzeichnung am Tatort in Bezug auf die Anlage anbrachte. Dem Beschuldigten war es jedenfalls zumutbar sich vor dem Einsatz der Anlage mit der Rechtslage (insbesondere in Bezug auf die Kennzeichnung) vertraut zu machen. Hierzu verwies das Bundesverwaltungsgericht auf die Leitlinien des Europäischen Datenschutzausschusses 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte vom 10.07.2019, S. 21 ff.²⁰ Auch zu dieser Strafbestimmung hatte das Bundesverwaltungsgericht keine Bedenken hinsichtlich der ausreichenden Bestimmtheit und verwies auf die Judikatur des Verfassungsgerichtshofs zum Güterbeförderungsgesetz im Kontext einer Blankettstrafnorm.²¹

Die Revision wurde für zulässig erklärt, eine solche wurde erhoben.

Erkenntnis des Bundesverwaltungsgerichts vom 19.11.2021, GZ: W211 2236448-1

Das Bundesverwaltungsgericht hat mit gegenständlichem Erkenntnis einer Beschwerde teilweise Folge gegeben und die Strafe reduziert, ansonsten wurde die Beschwerde als unbegründet abgewiesen bzw. das Straferkenntnis der Datenschutzbehörde dem Grunde nach bestätigt.

Die Datenschutzbehörde verhängte eine Geldbuße wegen unrechtmäßiger Verarbeitung personenbezogener Daten. Der Verantwortliche lud einen - von ihm mittels einer „Dash-Cam-Anlage“ aufgezeichneten - Verkehrsunfall auf der Plattform „Youtube“ hoch. Auf diesem Video waren die Kennzeichen eines Unfallbeteiligten sowie unbeteiligter Fahrzeuge zu erkennen. Der Verantwortliche führte ins Treffen, dass er das Video per Link an das Innenministerium als Beweismittel schicken wollte, um das Vorgehen der zuständigen Sicherheitsbehörde zu monieren.

20 Online abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_de.

21 Vgl. VfGH, VfSlg. 17.479, 04.03.2005.

Das Bundesverwaltungsgericht stellte zwar fest, dass das Video auf Youtube als „privat“ hochgeladen wurde und daher nur jene Personen, die den Link zum Video kannten, das Video auch tatsächlich aufrufen konnten. Dennoch ging das Bundesverwaltungsgericht von einer Verarbeitung (Offenlegung durch Verbreitung) aus. Das Bundesverwaltungsgericht führte hierzu ins Treffen, dass die Größe der Gruppe an Personen, die das Video aufgerufen haben, für das Vorliegen einer Verarbeitung irrelevant ist.

Der Beschuldigte stützte die Verarbeitung auf berechnigte Interessen gemäß Art. 6 Abs. 1 lit. f DSGVO. Die Verarbeitung war im Ergebnis jedoch nicht erforderlich für die Gewährleistung der Interessen des Beschuldigten, da nicht das gelindeste Mittel gewählt wurde. Das Video hätte auch mittels einer DVD an das Innenministerium übermittelt werden können. Eine DVD hätte die allfällige Weitergabe des Videos an Dritte deutlich erschwert, ein Link könnte leichter und unkontrolliert an Dritte weitergegeben werden. Darüber hinaus hätte der Beschuldigte die Kennzeichen sämtlicher unbeteiligter Verkehrsteilnehmer unkenntlich machen müssen.

Der Beschuldigte monierte im Rahmen seiner Beschwerde zudem, dass im Spruch des Straferkenntnisses der Hauptwohnsitz des Beschuldigten als Tatort angeführt wurde. Tatsächlich habe er das Video jedoch nicht von seinem Hauptwohnsitz auf Youtube hochgeladen. Das BVwG hielt in diesem Zusammenhang fest, dass der Spruch im Straferkenntnis in Bezug auf den Tatort (Hauptwohnsitz, jedoch jedenfalls in Österreich) im Sinne des § 44a Z 1 VStG ausreichend bestimmt ist. Es lagen keine Hinweise vor, dass die Tathandlung nicht in Österreich gesetzt wurde. Die konkrete Bezeichnung eines Ortes im Bundesgebiet war für die Wahrung der Verteidigungsrechte des Beschuldigten nicht erforderlich und es besteht auch keine Gefahr der Doppelbestrafung.²²

Die Strafe wurde reduziert, weil kein Vorsatz, sondern Fahrlässigkeit vorlag. Die Revision wurde für zulässig erklärt. Das Erkenntnis ist nicht rechtskräftig.

3.2.7 Verfahren über die Meldung der Verletzung des Schutzes personenbezogener Daten

Im Berichtsjahr wurden der Datenschutzbehörde 1.169 nationale Sicherheitsverletzungen („Data Breaches“) gemäß Art. 33 DSGVO gemeldet.

Dazu kamen 30 Meldungen betreffend grenzüberschreitender Sicherheitsverletzungen sowie 62 Sicherheitsverletzungen, die an andere Aufsichtsbehörden im Unionsgebiet herangetragen und der Datenschutzbehörde aufgrund potentieller Betroffenheit im Sinne des Art. 4 Z. 22 DSGVO im Rahmen eines Verfahrens gemäß Art. 65 DSGVO zur Kenntnis gebracht wurden.

Von Betreibern öffentlicher Kommunikationsdienste wurden 55 Sicherheitsverletzungen nach § 164 TKG 2021 gemeldet. Gemäß § 164 TKG 2021 hat im Fall einer Verletzung des Schutzes personenbezogener Daten oder der nicht öffentlich zugänglichen Daten einer juristischen Person unbeschadet des § 44 sowie unbeschadet der Bestimmungen des DSG und der DSGVO der Betreiber öffentlicher Kommunikationsdienste unverzüglich die Datenschutzbehörde von dieser Verletzung zu benachrichtigen.

Hervorzuheben ist, dass im Jahr 2021 eine nicht unwesentliche Anzahl gemeldeter Vorfälle auf die Covid-19-Pandemie zurückzuführen war, insbesondere im Zusammenhang mit den Covid-19-Testergebnissen.

22 Vgl. VwGH 01.04.2021, Ra 2021/05/0040.

Verstärkt sind auch Vorkommnisse im Zusammenhang mit Ransomware-Angriffen (Verschlüsselung von Daten durch Schadsoftware) an die Datenschutzbehörde gemeldet worden. In diesen Fällen werden die personenbezogenen Daten durch ein Programm verschlüsselt. Zumeist reicht dem Angreifer eine Verschlüsselung der Daten aus, ohne dass die Daten nach außen übertragen werden. Der nächste Schritt des Angreifers ist die Kontaktaufnahme mit dem betroffenen Unternehmen oder einer Einzelperson, um eine geldwerte Gegenleistung (bevorzugt in den Kryptowährungen Bitcoin oder Monero) für die Bekanntgabe des Entschlüsselungscodes zu verlangen.

Hierbei sind vor allem die Angriffe auf Microsoft Exchange Server zu erwähnen, wodurch sich die Angreifer gezielt eine temporäre Schwachstelle zu Nutze machten und eine Backdoor-Software installierten, die wiederum zum Hochladen und Ausführen anderer Programme verwendet worden ist.

Es kam auch vermehrt zum Versand von E-Mails bzw. Schreiben an falsche Empfänger. Dies war zumeist auf menschliche Fehler zurückzuführen. In solchen Fällen sind die Optionen des Verantwortlichen sehr begrenzt und es empfiehlt sich daher, präventiv zu arbeiten, beispielsweise durch das Einführen eines Vier-Augen-Prinzips. Ebenso ist ein mehrstufiges Sicherheitssystem bei elektronischen Geräten wie Notebooks oder Handys sinnvoll, um im Falle eines Verlustes oder Diebstahls einen unbefugten Zugriff zu unterbinden bzw. zumindest zu erschweren. Auf erster Ebene, dass das jeweilige Benutzerkonto geschützt ist, auf zweiter Ebene eine passwortgeschützte Festplatte.

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.

Die Daten, welche der Angreifer durch einen Identitätsdiebstahl erlangen könnte, können beispielsweise, sofern es sich um Zahlungsdaten handelt, für unbefugte Zahlungen im Internet verwendet werden.

Falls die Datenschutzbehörde feststellen sollte, dass bei einer Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die betroffene Person vorliegt und der / die Verantwortliche aufgrund seiner / ihrer Risikoanalyse zu einem konträren Ergebnis gelangt ist, kann die Datenschutzbehörde den Verantwortlichen entsprechend Art. 58 Abs. 2 lit. e DSGVO anweisen, eine nach Art. 34 Abs. 1 DSGVO gebotene Benachrichtigung nachzuholen oder bei Gefahr in Verzug einen Mandatsbescheid im Sinne des § 22 Abs. 4 DSGVO erlassen.

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 2021 wurde die Datenschutzbehörde als Aufsichtsbehörde in einem Fall gemäß Art. 36 DSGVO konsultiert. Der Verantwortliche plante 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 der Antrag auf Konsultation nach Art. 36 DSGVO abgewiesen.

Die verantwortliche Antragstellerin war der Ansicht, dass ein hohes Risiko für die Effektivität der Erfüllung der Informationspflichten durch die Kennzeichnung vorläge, da die betroffenen Personen von der Datenverarbeitung in Form einer Videoüberwachung in ihrem privaten oder beruflichen Lebensbereich erfasst werden würden und nicht derart rechtzeitig über die Datenverarbeitung informiert werden würden, um der Anwendung auszuweichen und eine alternative Route wählen.

Bei der Kennzeichnung der gegenständlichen Videoüberwachung handelte es sich um entsprechende Hinweisschilder, gut sichtbar, in der Nähe der gesicherten Brücken mit dem Namen der Verantwortlichen, einem QR-Code und dem Weblink zu der Datenschutzerklärung der Verantwortlichen.

In der Entscheidung setzte sich die Datenschutzbehörde mit dem Begriff des „hohen Risikos“ auseinander. Die Datenschutzbehörde folgt hierbei dem ErwGr 89 der DSGVO, welcher hervorhebt, dass es sich hierbei insbesondere um Verarbeitungsvorgänge handelt, bei denen neue Technologien eingesetzt werden oder die neuartig sind.

Bei Bildverarbeitungen sehen die Leitlinien 3/2019 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten durch Videogeräte hinsichtlich der zu erteilenden Information ein Zwei-Stufen Modell vor.

Die Informationen der ersten Ebene (Hinweisschild) sollten in der Regel die wichtigsten Informationen enthalten, z. B. Angaben zu den Zwecken der Verarbeitung, zur Identität des Verantwortlichen und zum Bestehen der Rechte der betroffenen Person sowie weitere Informationen mit hoher Bedeutung.

Informationen der zweiten Ebene müssen ebenfalls an einem für die betroffene Person leicht zugänglichen Ort zur Verfügung gestellt werden. Darüber hinaus ist es am besten, wenn die Informationen der ersten Ebene auf eine digitale Quelle (z. B. QR-Code oder Internetadresse) der zweiten Ebene verweisen.

Die von der Verantwortlichen vorgesehene Kennzeichnung war sowohl von der geplanten örtlichen Positionierung als auch vom Inhalt her eine geeignete Maßnahme, um das identifizierte

Risiko zu minimieren. Sie entsprach dem Modell, welches in Leitlinien 3/2019 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten durch Videogeräte empfohlen wird.

Daher wurde nach einer allumfassenden Interessensabwägung im Sinne des Art. 5 iVm Art. 6 DSGVO die Zulässigkeit der gegenständlichen Datenverarbeitung bejaht, da das von der Verantwortlichen aufgeworfene „hohe Restrisiko“ durch die geplanten Aufnahme-, Auswertungs- und Löschmodalitäten derart stark reduziert wurde, dass im Ergebnis kein hohes Restrisiko für Betroffene erkannt werden konnte.

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 acht Verhaltensregeln genehmigt, davon sind drei nach wie vor unter der aufschiebenden Bedingung genehmigt, dass in weiterer Folge eine Überwachungsstelle gemäß Art. 41 Abs. 2 DSGVO akkreditiert wird.

Bei den nachfolgenden fünf wurde bereits eine dazugehörige Überwachungsstelle gemäß Art. 41 Abs. 2 DSGVO akkreditiert:

- Verhaltensregeln für Internet Service Provider;
- Verhaltensregeln für die Ausübung des Gewerbes der Adressverlage und Direktmarketingunternehmen gem. § 151 Gewerbeordnung 1994;
- Verhaltensregeln für Netzbetreiber bei der Verarbeitung von mit intelligenten Messgeräten erhobenen personenbezogenen Daten von Endverbrauchern nach den §§ 83 ff. ElWOG 2010;
- Verhaltensregeln für Bilanzbuchhaltungsberufe (Bilanzbuchhalter, Buchhalter, Personalverrechner);
- Verhaltensregeln zum Datenschutz der Berufsvereinigung der ArbeitgeberInnen privater Bildungseinrichtungen.

Eine Aufzählung findet sich auf der Website der Datenschutzbehörde.²³ Darüber hinaus hat auch der Europäische Datenschutzausschuss ein Register von Verhaltensregeln aller Mitgliedstaaten veröffentlicht, welches laufend ergänzt wird.²⁴

Auf der Website befindet sich ein „Frage und Antworten“ Bereich zum Thema „Verhaltensregeln und Überwachungsstellen“.²⁵

In diesem Bereich wird auch auf die praxisrelevante Frage eingegangen, ob es mehrere Überwachungsstellen für dieselben Verhaltensregeln geben kann. Die Datenschutzbehörde geht – im Einklang mit den Leitlinien des EDSA (siehe unten) – davon aus, dass es für dieselben branchen-

23 Verzeichnis gemäß Art. 40 Abs. 6 DSGVO unter Verzeichnis der genehmigten Verhaltensregeln - Datenschutzbehörde (dsb.gv.at).

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

25 <https://www.dsb.gv.at/aufgaben-taetigkeiten/genehmigung-von-verhaltensregeln.html>.

spezifischen 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).

Darüber hinaus hat die Datenschutzbehörde ausgesprochen, dass Verhaltensregeln, die faktisch nur für ein Unternehmen gelten würden, nicht genehmigungsfähig sind (vgl. dazu mit näherer Begründung den Newsletter 1/2022).

Weiterführende Informationen zu diesem Thema sind auch in den Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679 des EDSA zu finden.²⁶

3.2.10 Verhängung von Geldbußen durch die Österreichische Datenschutzbehörde: Erfahrungs- und Vollzugsbericht 2021

Die Österreichische Datenschutzbehörde ist nach § 22 Abs. 5 DSG als nationale Aufsichtsbehörde für die Verhängung von Geldbußen gemäß Art. 58 Abs. 2 lit. i DSGVO für Verstöße gegen die bußgeldbewehrten Bestimmungen nach Art. 83 DSGVO und (subsidiär) § 62 DSG sowohl gegenüber natürlichen als auch juristischen Personen zuständig. Auch im Jahr 2021 bildeten die Verfahren gegen natürliche Personen den größeren Bestandteil der Verwaltungsstrafverfahren.

Die Datenschutzbehörde hat - in diesem Zusammenhang - im Beobachtungszeitraum 36 Geldbußen (11 davon gegenüber juristischen Personen) sowie sieben Verwarnungen ausgesprochen. Insgesamt hat die Datenschutzbehörde im Jahr 2021 Geldbußen in Höhe von circa EUR 24.700.000,00 verhängt. Darüber hinaus erfolgten noch mehrere Bescheide im Rahmen von Anträgen auf Wiedereinsetzung, auf Einräumung von Parteiengehör u.ä. Hinsichtlich der Anzahl von Verwaltungsstrafverfahren wird auf Punkt 3.1 („Statistische Darstellung“) verwiesen.

Zu den Verwaltungsstrafverfahren gegen natürliche Personen

Unrechtmäßige Bildverarbeitung durch Private

Wie auch schon in den Vorjahren stellten die Verfahren gegen natürliche Personen wegen des unrechtmäßigen Betriebs einer Bildverarbeitungsanlage bzw. Videoüberwachungsanlage (z.B. ausgehend von privaten Gebäuden sowie aus Fahrzeugen heraus in Form von sogenannten „Dash-Cams“) einen wesentlichen Teil der von der Datenschutzbehörde geführten Verwaltungsstrafverfahren dar.

Der Einsatz solcher Bildverarbeitungsanlagen durch Private ist nicht per se unzulässig, jedoch führten die gewählten Einstellungen im Einzelfall dazu, dass ein unberechtigter Eingriff in die Grundrechte betroffener Personen erfolgte. Im Regelfall lag ein Verstoß gegen die Datenverarbeitungsgrundsätze des Art. 5 Abs. 1 lit. a und c DSGVO vor, da der Aufnahmebereich der Anlage und/oder die Speicherdauer der Aufzeichnungen nicht auf das gelindeste Mittel beschränkt wurden. Die jeweils verfolgten Zwecke bzw. berechtigten Interessen der Verantwortlichen gemäß Art. 6 Abs. 1 lit. f DSGVO (Schutz des Eigentums und Gesundheit) hätten mit einem Aufnahmebereich, der keinen öffentlichen Raum erfasst, und einer Speicherdauer, die nicht über 72 Stunden liegt, gewährleistet werden können.

²⁶ https://www.dsb.gv.at/europa-internationales/europaeischer_datenschutzausschuss_edsa.html.

Darüber hinaus wurden Bildverarbeitungsanlagen durch die Verantwortlichen in etlichen Fällen auch nicht geeignet gekennzeichnet, sodass die Betroffenen nicht rechtzeitig über die Bild-datenverarbeitung informiert wurden. Auf Grund der Informationsmenge, die einem/einer Be-troffenen zukommen soll, kann von einem/einer Verantwortlichen ein "geschichteter Zugang" und eine Kombination aus Mitteln gewählt werden, um dem Transparenzgebot zu entsprechen. Im Rahmen einer Videoüberwachung sollte die wichtigste Information in einem Warnhinweis dargestellt werden, während die notwendigen weiteren Informationen mit anderen Mitteln zur Verfügung gestellt werden können (sozusagen als zweite Schicht) (vgl. Europäischer Da-tenschutzausschuss, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Vi-deogeräte, 29.01.2020, S. 28 ff, online abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_de).

Unrechtmäßige Verarbeitung von Gesundheitsdaten

Eine natürliche Person (im Folgenden „Beschuldigter“) schrieb eine Nachricht per E-Mail an eine öffentliche Einrichtung und wollte diese darauf aufmerksam machen, dass die Aussage einer Kindergärtnerin, die öffentlich bekannt gab, zu 50% behindert zu sein, nicht der Realität entspreche. Hierzu übermittelte der Beschuldigte ein Gerichtsgutachten im Anhang. Dieses Ge-richtsgutachten erhielt der Beschuldigte ursprünglich als Partei im Rahmen eines zivilgericht-lichen Verfahrens. Das Dokument beinhaltete gesundheitsbezogene Daten der Betroffenen.

Die Datenschutzbehörde stellte im Ergebnis fest, dass die gegenständliche Übermittlung des Gutachtens eine unrechtmäßige Verarbeitung sensibler Daten darstellte, da die konkrete Ver-arbeitung auf keine Rechtsgrundlage im Sinne des Art. 9 Abs. 2 DSGVO gestützt werden konnte. Es lag somit eine Verwaltungsübertretung nach Art. 5 Abs. 1 lit. a iVm Art. 9 Abs. 1 und Abs. 2 iVm Art. 83 Abs. 1 und Abs. 5 lit. a DSGVO vor und die Datenschutzbehörde verhängte eine Geldbuße in Höhe von **EUR 600,00**.

Zu den Verwaltungsstrafverfahren gegen juristische Personen

Das Kammergericht Berlin ersuchte den EuGH um Auslegung des Art. 83 DSGVO in Bezug auf die Frage, ob ein Unternehmen unmittelbar Beschuldigter im Bußgeldverfahren wegen eines Verstoßes gegen Art. 83 DSGVO sein kann und wenn ja, ob für die Verhängung einer Geldstrafe nach dem „strict-liability-Grundsatz“ bereits ein dem Unternehmen zuzuordnender objektiver Pflichtenverstoß ausreicht.

In Reaktion auf das mit Beschluss vom 06.12.2021 vom Kammergericht Berlin initiierte Vor-abentscheidungsverfahren nach Art.267 AEUV (beim EuGH unter der GZ: C-807/21 derzeit anhängig) setzt die Datenschutzbehörde gemäß § 24 VStG iVm § 38 AVG sämtliche Verwal-tungsstrafverfahren gegen juristische Personen im jeweiligen Verfahrensstatus aus, soweit kei-ne weiteren Ermittlungsschritte erforderlich oder die Verfahren gegebenenfalls nicht ohnehin einzustellen sind.

Unzulässige Einwilligungen/Verarbeitung im Rahmen von Kundenbindungsprogrammen

Die Datenschutzbehörde hat im Jahr 2021 insgesamt drei Geldbußen gegen juristische Per-sonen, die in Österreich Kundenbindungsprogramme betreiben und für die Verarbeitung von personenbezogenen Daten zum Zwecke des Profiling von den Betroffenen eine Einwilligung erhoben, verhängt. Die Einwilligungen wurden entweder im Rahmen eines physischen Flyers oder elektronisch auf der Webseite der Verantwortlichen erhoben.

Es ist entscheidend, dass bei der Verarbeitung von personenbezogenen Daten auf Grund einer Einwilligung des Betroffenen im Sinne des Art. 6 Abs. 1 lit. a DSGVO jedenfalls die Bedingungen

einer Einwilligung nach Art. 7 DSGVO erfüllt sein müssen. Werden diese nicht erfüllt, liegt eine unzulässige Einwilligung der Betroffenen vor und die Datenverarbeitung ist in Folge mangels Rechtsgrundlage zu unterlassen. Darüber hinaus führt eine unzulässige Einwilligung dazu, dass die Datenverarbeitung rückwirkend als unrechtmäßig zu qualifizieren ist.

In den Verwaltungsstrafverfahren gegen die Unternehmen wurde zusammengefasst festgestellt, dass sowohl die Formulare für die Erhebung der Einwilligungen mittels Flyer als auch auf der Webseite irreführend gestaltet waren, sodass der Durchschnittsnutzer bei der Erteilung der Einwilligung nicht erkennen konnte, dass er auch eine Einwilligung für Profiling erteilt. Auf Grund der irreführenden Gestaltung der Einwilligungsformulare stellte die Datenschutzbehörde daher im Ergebnis fest, dass die erhobenen Einwilligungen der Betroffenen unzulässig waren. Die Verantwortlichen stützten die Verarbeitung ausschließlich auf diese unzulässige Einwilligung. Die Datenschutzbehörde stellte daher zudem fest, dass die bisherige Datenverarbeitung - mangels Rechtsgrundlage - unrechtmäßig erfolgte.

Die Datenschutzbehörde untersagte - im Rahmen von amtswegigen Prüfverfahren - nicht nur die Datenverarbeitung, die auf Grund der unzulässigen Einwilligung bis dahin erfolgte, sondern verhängte gegen die jeweiligen Verantwortlichen Geldbußen in Höhe von insgesamt **EUR 11.200.000,00**. Diese Straferkenntnisse sind nicht rechtskräftig.

Verstoß gegen den Erleichterungsgrundsatz

Gemäß Art. 12 Abs. 2 DSGVO müssen Verantwortliche den Betroffenen die Ausübung ihrer Rechte gemäß den Art. 15 bis 22 DSGVO erleichtern.

Die Verantwortliche hat in einem festgestellten Zeitraum von mehr als einem Jahr gegen den Erleichterungsgrundsatz nach Art. 12 Abs. 2 DSGVO verstoßen, indem sie ein Kontaktformular auf ihrer Webseite für die Behandlung von elektronischen Betroffenenanfragen zur Geltendmachung von Betroffenenrechten implementierte und ab diesem Zeitpunkt die Betroffenen im Rahmen des elektronischen Kanals systematisch auf die ausschließliche Nutzung des Formulars verwies. Das von den Betroffenen zuvor für die Geltendmachung ihrer Rechte genutzte E-Mail-Postfach wurde mit der Implementierung des Kontaktformulars in Folge derart umgestellt, dass sämtliche E-Mails an dieses Postfach automatisiert mit einem Verweis auf die ausschließliche Nutzung eines neu implementierten Kontaktformulars auf der Webseite „beantwortet“ wurden. Die Verantwortliche überprüfte dieses Postfach nur mehr auf Eingänge der Datenschutzbehörde, ansonsten wurde das vom überwiegenden Teil der Betroffenen genutzte Postfach ignoriert. Bis zur Implementierung des Kontaktformulars waren E-Mails das von der überwiegenden Mehrheit der Betroffenen genutzte Kommunikationsmittel zur Ausübung der Betroffenenrechte (circa 98% der Betroffenenanfragen wurden bei der Verantwortlichen mittels einer E-Mail eingebracht).

Betroffene, die bereits in den Tagen, Wochen oder Monaten vor der Umstellung auf das Kontaktformular einen Antrag per E-Mail übermittelten und sich daher in Korrespondenz mit der Verantwortlichen befanden, wurden schließlich dazu aufgefordert einen gänzlich neuen Antrag über ein von der Verantwortlichen vorgegebenes Kontaktformular einzubringen. Im Rahmen des Kontaktformulars konnten die Betroffenen zudem nur drei spezifische (von der Verantwortlichen vorgegebene) Betroffenenrechte ausüben.

Die Datenschutzbehörde stellte daher im Ergebnis fest, dass die Verantwortliche den elektronischen Eingangskanal für Betroffenenanfragen de facto auf ein von ihr vorgegebenes Kontaktformular eingeschränkt hat. Viele Betroffene befanden sich bereits seit mehreren Monaten in Korrespondenz und wurden plötzlich dazu aufgefordert, sich wieder „hinten anzustellen“

und das neue Kontaktformular zu verwenden. Die per E-Mail eingebrachten Anfragen der Betroffenen wurden ignoriert und nicht weiter behandelt. Dies führte jedoch dazu, dass die Betroffenen keinen neuen Antrag über das Formular, sondern vielmehr eine Beschwerde bei der Datenschutzbehörde einbrachten. Dem Gebot der Erleichterung entspricht es jedenfalls nicht, wenn Betroffene, die legitimer Weise Rechte ausüben wollen, gleichsam „im Kreis“ geschickt werden und eine Behandlung nur dann erfolgt, wenn Betroffene ausreichende Hartnäckigkeit beweisen. Die im vorliegenden Fall verhängte Geldbuße betrug **EUR 9.500.000,00** (nicht rechtskräftig).

Zusatz: Die Datenschutzbehörde hat grundsätzlich keine Bedenken gegen den Einsatz von Web-Formularen zur Kontaktaufnahme durch Betroffene, dies darf jedoch nicht dazu führen, dass sonstige Kommunikationswege (wie z.B. E-Mails) beschränkt oder sogar gänzlich ausgeschlossen werden.

Mangelnde Sicherheit der Verarbeitung

Die Datenschutzbehörde stellte in einem Verfahren fest, dass eine Verantwortliche in der Finanzbranche (Kreditinstitut) eine **Excel-Datei** zum Zwecke der internen Verwendung/Administration von Bankkunden, die personenbezogene Daten und insbesondere die Kontoinformationen der Kunden enthielt, filialweise auf einem internen Laufwerk gespeichert bzw. aufbewahrt hat. Die Datei konnte von allen Filial-Bediensteten bei Bedarf abgerufen und eingesehen werden. Die Excel-Datei war weder verschlüsselt, noch sonst durch andere adäquate Maßnahmen vor unberechtigten Zugriffen geschützt sowie gegen unbeabsichtigte Offenlegung gegenüber Dritten gesichert. In Folge wurde in einer von der Verantwortlichen betriebenen Filiale durch eine Mitarbeiterin eine E-Mail-Nachricht an 234 Kunden versendet. Dieser E-Mail schloss die Mitarbeiterin irrtümlich die oben genannte Excel-Liste an.

Die Datenschutzbehörde stellte im Rahmen des Verfahrens fest, dass sich in der Excel-Datei Datensätze von 5.971 Kunden der Verantwortlichen befanden. Die E-Mail-Nachricht wurde in 227 Fällen erfolgreich zugestellt, wodurch folgende Datenkategorien den 227 Empfängern der Nachricht offengelegt wurden: Kundenkurzbezeichnung, Adressdaten und Erreichbarkeiten, Alter und Geburtsdatum, Einkommen, Produktbesitz, Volumen je Produkt, Nutzung von Bankservices, Name und Abteilung der Betreuerin, betriebswirtschaftliche und bankorganisatorische Kennzeichnung des jeweiligen Kunden.

Die Verantwortliche hat daher im Ergebnis gegen den in Art. 5 Abs. 1 lit. f DSGVO normierten Grundsatz der Integrität und Vertraulichkeit sowie gegen ihre Pflicht zur Implementierung von geeigneten technischen und organisatorischen Sicherheitsmaßnahmen gemäß Art. 32 DSGVO verstoßen.

Die Datenschutzbehörde verhängte daher gegen das Kreditinstitut eine Geldbuße in der Höhe von **EUR 4.000.000,00** (nicht rechtskräftig).

Verstoß gegen die Mitwirkungspflicht von Verantwortlichen

Verantwortliche sowie Auftragsverarbeiter und gegebenenfalls deren Vertreter sind gemäß Art. 31 DSGVO auf Anfrage zur Zusammenarbeit mit der Aufsichtsbehörde zum Zwecke der Erfüllung ihrer Aufgaben verpflichtet.

Im konkreten Fall wurden bei der Datenschutzbehörde drei Beschwerden von unterschiedlichen Betroffenen gegen eine Verantwortliche eingebracht (ehemalige Arbeitnehmer der Verantwortlichen). Im Rahmen dieser Beschwerdeverfahren wurde die Verantwortliche als Beschwerdegegnerin dazu aufgefordert, binnen einer bestimmten Frist eine Stellungnahme

zur Beschwerde der Betroffenen in den jeweiligen Verfahren bei der Datenschutzbehörde einzubringen. Die Verantwortliche hat jedoch in Folge gegen ihre Pflicht gemäß Art. 31 DSGVO zur **Zusammenarbeit mit der Datenschutzbehörde** als Aufsichtsbehörde verstoßen, indem sie in den drei separaten Beschwerdeverfahren als Beschwerdegegnerin beteiligt war und trotz Urgenz durch die Datenschutzbehörde sich weigerte am Verfahren teilzunehmen bzw. eine Stellungnahme einzubringen. Die Verantwortliche hat sich in Bezug auf zwei Beschwerden überhaupt nicht und in einem Fall erst stark verspätet zum Vorbringen des Beschwerdeführers geäußert.

Die Datenschutzbehörde stellte daher im Ergebnis eine Verletzung von Art. 31 iVm Art. 83 Abs. 4 lit. a DSGVO fest und verhängte eine Geldbuße in Höhe von **EUR 3.000,00**.

3.2.11 Stellungnahmen zu Gesetzes- und Verordnungsentwürfen

Die Datenschutzbehörde hat im Jahr 2021 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.

- Entwurf eines Bundesgesetzes, mit dem das BekGG und das IslamG geändert werden
- -Terror-Bekämpfungsgesetz – TeBG
- Telekommunikationsgesetz; KommAustria-Gesetz, Strafprozeßordnung u.a., Änderung
- Bundesgesetz, mit dem das Gerichtsorganisationsgesetz (GOG) und das Bundesverwaltungsgerichtsgesetz (BVwGG) geändert werden
- Bundesgesetz, mit dem das Arbeitsvertragsrechts-Anpassungsgesetz, das Arbeitsverfassungsgesetz, das Dienstnehmerhaftpflichtgesetz, das Arbeitsinspektionsgesetz 1993, das Allgemeine Sozialversicherungsgesetz, das Beamten-Kranken- und Unfallversicherungsgesetz und das Einkommensteuergesetz 1988 geändert werden (Homeoffice-Paket)
- 2. Kontenregister-Durchführungsverordnung
- Bundesgesetz, mit dem das Epidemiegesetz 1950 und das COVID-19-Maßnahmengesetz geändert werden
- Strafrechtliches EU-Anpassungsgesetz 2021
- Ärztegesetz-Novelle 2021
- Entwurf eines Bundesgesetzes, mit dem das Bundes-Verfassungsgesetz, das Rechnungshofgesetz 1948 und das Verfassungsgerichtshofgesetz 1953 geändert und ein Informationsfreiheitsgesetz erlassen werden
- Unterbringungsgesetz- und IPR-Gesetz-Novelle 2021
- Bundesgesetz, mit dem das Polizeiliche Staatsschutzgesetz, das Sicherheitspolizeigesetz, das Strafgesetzbuch, die Strafprozessordnung 1975 und das Tilgungsgesetz 1972 geändert werden
- Kartell- und Wettbewerbsrechts-Änderungsgesetz 2021
- AWG-Novelle Kreislaufwirtschaftspaket
- Bundesgesetz, mit dem das Unternehmensserviceportalgesetz - USPG geändert wird
- Änderung des Vereinsgesetzes 2002 und des Waffengesetzes 1996 Bundesgesetz, mit dem das Epidemiegesetz 1950 und das COVID-19-Maßnahmengesetz geändert werden
- Transparenzdatenbank - Abfrageverordnung 2021
- Novelle des Luftfahrtgesetzes
- Bundesgesetz, mit dem das Ausschreibungsgesetz 1989 geändert wird
- Änderung des Bauarbeiter-Urlaubs- und Abfertigungsgesetzes
- Bundesgesetz, mit dem das Bundesgesetz betreffend Medizinprodukte 2021 (Me-

- dizinproduktegesetz 2021 – MPG 2021) erlassen und das Gesundheits- und Ernährungssicherheitsgesetz - GESG geändert werden
- Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung sowie der Bundesministerin für Landwirtschaft, Regionen und Tourismus, mit der die Bildungsdokumentationsverordnung 2021 geändert wird
 - Bundesgesetz, mit dem das Bundesstatistikgesetz 2000 und das Forschungsorganisationsgesetz geändert werden
 - Bundesgesetz, mit dem das Arzneimittelgesetz und das Gentechnikgesetz geändert werden
 - Bundesgesetz, mit dem ein Sterbeverfügungsgesetz erlassen und das Suchtmittelgesetz sowie das Strafgesetzbuch geändert werden
 - COVID-19-Impfpflichtgesetz
 - Ökosoziales Steuerreformgesetzes 2022 Teil 1
 - Ökosoziale Steuerreform Teil II Klimabonus
 - Gesetzesentwurf zum Gemeinde-Wasserleitungsgesetz NÖ
 - Entwurf eines Bundesgesetzes, mit dem das E-Government-Gesetz geändert wird

4 Wesentliche höchstgerichtliche Entscheidungen

Generell war das Berichtsjahr durch eine intensive Entscheidungstätigkeit der Höchstgerichte, sowohl auf nationaler wie auf internationaler Ebene, gekennzeichnet.

4.1 Verfahren vor dem Verfassungsgerichtshof

Im Berichtszeitraum sind folgende datenschutzrechtlich relevante Entscheidungen des Verfassungsgerichtshofes ergangen:

Erkenntnis vom 4.3.2021, E 4037/2020

In dieser in einer Grundrechtsbeschwerdesache gegen das Erkenntnis des BVwG vom 1.10.2020, Zl. W274 2227645-1, ergangenen Entscheidung hat der VfGH umfassende Erwägungen zur Abwägung der Grundrechte auf Datenschutz (§ 1 DSG) und Schutz des Privat- und Familienlebens (Art. 8 EMRK) gegen das Grundrecht auf Informationsfreiheit (Art. 10 EMRK) vorgenommen, wobei im Beschwerdefall (nach dem AuskunftspflichtG verweigerte Auskunft an einen Journalisten über Gehaltsfortzahlungen von aus dem Nationalrat ausgeschiedenen Mitgliedern) das Grundrecht auf Informationsfreiheit überwogen hat.

Das Erkenntnis des BVwG wurde aufgehoben

Erkenntnis vom 10.3.2021, V 573/2020

In diesem durch einen Individualantrag eingeleiteten Normenkontrollverfahren (Verordnungsprüfung) hat der VfGH Bestimmungen einer Verordnung des Magistrates der Stadt Wien betreffend die Auskunftserteilung über Kunden von Gastronomiebetrieben bei Verdachtsfällen von COVID-19 mangels nachvollziehbarer Dokumentation der Entscheidungsgrundlagen für gesetzwidrig erklärt (die Verordnung war im Entscheidungszeitpunkt bereits außer Kraft getreten). Die angewendeten, weitreichenden Verordnungsermächtigungen nach den §§ 5 und 5c EpiG würden schwerwiegende Eingriffe in das Grundrecht auf Datenschutz durch die Ermittlung von Kontaktpersonen und der Möglichkeit von Rückschlüssen auf die persönliche Lebensführung großer Teile der Bevölkerung ermöglichen. Da der Magistrat Wien als Verordnungsgeber keine nachvollziehbare Dokumentation seiner Entscheidungsgrundlagen vorgelegt hatte, fehlte es an der gebotenen Darlegung der für die Willensbildung des Verordnungsgebers ausschlaggebenden Motive.

Es handelte sich um jene Verordnung, die auch im Bescheid der DSB vom 19.11.2020, GZ: 2020-0.743.659 (Verfahrenszahl: DSB-D124.3093), anzuwenden gewesen wäre, von der DSB wegen offenkundigen Widerspruchs zu Unionsrecht aber unangewendet gelassen wurde (siehe Datenschutzbericht 2020, Seiten 30 f).

Erkenntnis vom 6.10.2021, UA 2/2021

In dieser Entscheidung in einer Beschwerdesache gemäß Art. 138b Abs. 1 Z 7 B-VG (Beschwerde wegen Verletzung von Persönlichkeitsrechten durch einen Untersuchungsausschuss des Nationalrats) hatte sich das Höchstgericht u.a. mit der Frage zu befassen, ob das Grundrecht

auf Datenschutz (§ 1 DSG) der Beschwerdeführerin (Aufsichtsratsmitglied einer staatsnahen GmbH) durch Fragen einer Abgeordneten im Ibiza-Untersuchungsausschuss des Nationalrats an zwei Auskunftspersonen, darunter den für die Bestellung der Beschwerdeführerin verantwortlichen früheren Bundesminister, verletzt wurde. Der VfGH kam dabei zu dem Schluss, dass Mitglieder von Aufsichtsräten weitergehende Kritik bzw. kritische Fragestellungen hinsichtlich Ausbildung, Kompetenz und Eignung für die Funktion als Mitglied eines Aufsichtsrates hinzunehmen haben als Privatpersonen. Die Aufzählung der Schul- und Berufsausbildung der Beschwerdeführerin im Zuge der Befragung war daher keine Verletzung im Recht auf Datenschutz und auf Achtung des Privat- und Familienlebens.

4.2 Oberster Gerichtshof

Der OGH hat im Berichtsjahr inhaltlich dreimal Vorabentscheidungsersuchen (Art. 267 AEUV) zur DSGVO an den EuGH gerichtet, die teilweise auch für die Entscheidungspraxis der DSB von hoher Relevanz sind. Er ist damit das bisher bei weitem vorlagefreudigste österreichische Höchstgericht.

Beschluss vom 18.2.2021, 6 Ob 159/20f

In diesem Zivilprozess betreffend das Auskunftsrecht gemäß Art. 15 DSGVO ist die Frage des Rechts auf Auskunftserteilung über bestimmte Empfänger oder allgemeine Empfängerkreise entscheidend. Die fallspezifische Vorlagefrage lautet:

„Ist Art. 15 Abs. 1 lit. c 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“) dahingehend auszulegen, dass sich der Anspruch auf die Auskunft über Empfängerkategorien beschränkt, wenn konkrete Empfänger bei geplanten Offenlegungen noch nicht feststehen, der Auskunftsanspruch sich aber zwingend auch auf Empfänger dieser Offenlegungen erstrecken muss, wenn Daten bereits offengelegt worden sind?“

Urteil vom 18.2.2021, 6 Ob 127/20z

Der Kläger hatte von einem Post-, Logistik- und Direktmarketingunternehmen Feststellung, Datenlöschung und Auskunftserteilung betreffend Daten zu ihm betreffenden Marketingklassifikationen begehrt. Das Berufungsgericht hatte der Klage teilweise stattgegeben und ausgesprochen, dass die Beklagte dem Kläger bei allfälligen Auskunftsverlangen über Daten zur Bioaffinität, Nachtschwärmereigenschaft, Heimwerkereigenschaft, Akademikereigenschaft, Lebensphase, Investment- und Distanzhandelsaffinität und Kinderlosigkeit des Klägers Auskunft im Sinn des Datenschutzgesetzes zu erteilen habe (Art. 15 Abs. 1 lit a bis g DSGVO).

Der OGH stellte dagegen das gänzlich abweisende Urteil des Erstgerichts wieder her. Er bekräftigte die – von der Beklagten bestrittene – Zuständigkeit der Zivilgerichte für Auskunftssachen (Art. 79 DSGVO), er hielt weiters (mit ausführlicher Begründung) fest, dass es sich bei errechneten Marketingklassifikationen um personenbezogene Daten handelt. § 151 Abs. 6 GewO regle nur die Verwendung von Marketinginformationen und Marketingklassifikationen, ändere aber nichts daran, dass es sich dabei um von der DSGVO erfasste personenbezogene Daten handelt.

Letztlich konnte daraus für den Standpunkt des Klägers aber nichts gewonnen werden. Die Beklagte hatte sowohl das Auskunftsbeghehen als auch das Löschungsbegehren erfüllt. Da weiters ein aufrechter Widerspruch des Klägers gegen die weitere Verarbeitung der Daten vorlag, durfte die Verantwortliche keine weiteren Daten verarbeiten. Damit mangelte es dem Kläger an einem rechtlichen Interesse für die begehrte und vom Berufungsgericht ausgesprochene Feststellung.

Beschluss vom 15.4.2021, 6 Ob 35/21x

In dieser Zivilprozesssache betreffend die Tätigkeit einer als Adressverlag und Direktmarketingunternehmen tätigen Gesellschaft, die Daten zur „Parteiaffinität“ des Klägers verarbeitete hatte, geht es um die Frage des Bestehens und der Bemessung eines Schadenersatzanspruchs gemäß Art. 82 DSGVO. Die fallspezifischen Vorlagefragen lauten:

1. *Erfordert der Zuspruch von Schadenersatz nach Art. 82 DSGVO (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]) neben einer Verletzung von Bestimmungen der DSGVO auch, dass der Kläger einen Schaden erlitten hat oder reicht bereits die Verletzung von Bestimmungen der DSGVO als solche für die Zuerkennung von Schadenersatz aus?*
2. *Bestehen für die Bemessung des Schadenersatzes neben den Grundsätzen der Effektivität und Äquivalenz weitere Vorgaben des Unionsrechts?*
3. *Ist die Auffassung mit dem Unionsrecht vereinbar, dass Voraussetzung für den Zuspruch immateriellen Schadens ist, dass eine Konsequenz oder Folge der Rechtsverletzung von zumindest einigem Gewicht vorliegt, die über den durch die Rechtsverletzung hervorgerufenen Ärger hinausgeht?*

(Teil-) Urteil vom 23.6.2021, 6 Ob 56/21k

Der Kläger begehrte vom Betreiber eines digitalen sozialen Netzwerks (mit DSGVO-relevanter Niederlassung in Irland) u.a. die Feststellung der Abgrenzung der jeweiligen Rollen als Verantwortlicher und Auftragsverarbeiter, Unterlassung bestimmter Datenverarbeitungen, Auskunftserteilung und Zahlung von 500 EUR aus dem Titel des Schadenersatzes. Das ergangene Teilurteil befasst sich vor allem mit Aspekten des Schadenersatzes.

Verantwortlicher ist laut OGH jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle (personenbezogener Aspekt), die allein oder gemeinsam mit anderen (pluralistische Kontrolle), über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Beim Verantwortlichen handelt es sich um jene Person oder Einrichtung, die dafür zu sorgen hat, dass die Datenschutzbestimmungen der DSGVO eingehalten werden. Dies treffe auf die beklagte Gesellschaft (LL.C. nach irischem Recht) zu.

Laut OGH ist die Schadenersatzfrage allein nach Art. 82 DSGVO unionsrechtlich und ohne Bezug auf das nationale Recht zu beurteilen. Nicht nur der Begriff des „immateriellen Schadens“ in Art. 82 Abs. 1 DSGVO ist unionsautonom zu bestimmen, sondern auch die Ausgestaltung der sonstigen Haftungsvoraussetzungen nach Art. 82 Abs. 2 DSGVO und Fragen der Bemessung des Ersatzanspruchs.

Ungeachtet des unionsrechtlichen Effektivitätsgrundsatzes gebührt **Schadenersatz nur dann, wenn** ein (ideeller) **Schaden tatsächlich eingetreten** ist, wobei eine Rechtsverletzung allein noch keinen Schaden darstellt.

Eine Konsequenz oder Folge der Rechtsverletzung kann jedoch als immaterieller Schaden qualifiziert werden, wenn es sich um eine über den an sich durch die Rechtsverletzung hervorgerufenen Ärger bzw. Gefühlsschaden hinausgehende Beeinträchtigung handelt. Auch **Nachteile von geringem Gewicht** stellen dabei einen **ersatzfähigen Schaden** dar. Dabei reichte es im entschiedenen Fall aus, dass der Kläger „massiv genervt“ war.

Es wurde dafür ein Schadenersatz in Höhe von 500 EUR zugesprochen.

Beschluss vom 23.6.2021, 6 Ob 56/21k

In der bereits bekannten Zivilprozesssache sind weiters betreffend die Klagebegehren auf Feststellung, Unterlassung und Vertragsabschluss, u.a. die Grundsätze der Datenverarbeitung, die Rechtfertigungsgründe für die Datenverarbeitung und die Gültigkeit eingeholter Einwilligungen durch den Betreiber eines digitalen sozialen Netzwerks (mit DSGVO-relevanter Niederlassung in Irland) als Grundlagen für Online-Werbung von entscheidender Bedeutung.

Der OGH hat daher folgende Fragen (betreffend den Rest der Sache ist das vorstehende Teil- und Endurteil ergangen) zur Auslegung von Kernbestimmungen der DSGVO dem EuGH zur Vorabentscheidung vorgelegt:

1. *Sind die Bestimmungen der Art. 6 Abs. 1 lit a und b DSGVO dahingehend auszulegen, dass die Rechtmäßigkeit von Vertragsbestimmungen in allgemeinen Nutzungsbedingungen über Plattformverträge wie jenem im Ausgangsverfahren (insbesondere Vertragsbestimmungen wie: „Anstatt dafür zu zahlen [...] erklärst du dich durch Nutzung der F*****-Produkte, für die diese Nutzungsbedingungen gelten, einverstanden, dass wir dir Werbeanzeigen zeigen dürfen ... Wir verwenden deine personenbezogenen Daten [...] um dir Werbeanzeigen zu zeigen, die relevanter für dich sind.“), die die Verarbeitung von personenbezogenen Daten für Aggregation und Analyse von Daten zum Zwecke der personalisierten Werbung beinhalten, nach den Anforderungen des Art. 6 Abs. 1 lit a iVm Art. 7 DSGVO zu beurteilen sind, die nicht durch die Berufung auf Art. 6 Abs. 1 lit b DSGVO ersetzt werden können?*
2. *Ist Art. 5 Abs. 1 lit c DSGVO (Datenminimierung) dahin auszulegen, dass alle personenbezogenen Daten, über die eine Plattform wie im Ausgangsverfahren verfügt (insbesondere durch den Betroffenen oder durch Dritte auf und außerhalb der Plattform), ohne Einschränkung nach Zeit oder Art der Daten für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet werden können?*
3. *Ist Art. 9 Abs. 1 DSGVO dahin auszulegen, dass er auf die Verarbeitung von Daten anzuwenden ist, die eine gezielte Filterung von besonderen Kategorien personenbezogener Daten wie politische Überzeugung oder sexuelle Orientierung (etwa für Werbung) erlaubt, auch wenn der Verantwortliche zwischen diesen Daten nicht differenziert?*
4. *Ist Art. 5 Abs. 1 lit b iVm Art. 9 Abs. 2 lit e DSGVO dahin auszulegen, dass eine Äußerung über die eigene sexuelle Orientierung für die Zwecke einer Podiumsdiskussion die Verarbeitung von anderen Daten zur sexuellen Orientierung für Zwecke der Aggregation und Analyse von Daten zum Zwecke der personalisierten Werbung erlaubt?*

4.3 Verwaltungsgerichtshof

Betreffend die im Jahr 2020 vom VwGH ohne Vorlage an den EuGH entschiedene Frage der **verwaltungsstrafrechtlichen Verantwortung von Verbänden** (insbesondere juristischen Personen) und deren Leitungsorganen (Erkenntnis vom 12.5.2020, Ro 2019/04/0229, Datenschutzbericht 2020, Seite 53) wurde Ende 2021, nach mehreren divergenten Entscheidungen in der deutschen Rechtsprechung bei einer der österreichischen (§ 30 DSGVO) sehr ähnlichen einfachgesetzlichen Rechtslage (§ 30 dt. OWiG), durch ein deutsches Rechtsmittelgericht ein Vorabentscheidungsersuchen an den EuGH gerichtet (Kammergericht Berlin, Beschluss vom 6.12.2021, AZ: 3 Ws 250/21, EuGH Rs C-807/21). Für die DSB und das BVwG besteht damit die Möglichkeit, anhängige Verwaltungsstrafverfahren gemäß § 38 AVG bis zur Entscheidung des EuGH auszusetzen bzw. – soweit es sich um das BVwG handelt – den EuGH mit einem Vorabentscheidungsersuchen zu befassen

Erkenntnis vom 23.2.2021, Ra 2019/04/0054

Diese Entscheidung betrifft einen langjährigen, bereits mehrfach beide Höchstgerichte des öffentlichen Rechts beschäftigenden Verfahrenskomplex. Mit Bescheid vom 11.7.2016 hatte die DSB die datenschutzrechtliche Beschwerde der Revisionswerberin gegen das Bundesministerium für Inneres (BMI) wegen Verletzung im Recht auf Geheimhaltung durch Übermittlung einer Niederschrift an das Bundeskanzleramt abgewiesen. Diese Niederschrift sollte als Beweismittel in einem Beschwerdeverfahren gegen Österreich beim Hochkommissariat für Menschenrechte der Vereinten Nationen dienen, das die Revisionswerberin angestrengt hatte. Das BVwG bestätigte den Bescheid im Erkenntnis vom 14.3.2019, W256 2131983-1.

Die ao. Revision der Beschwerdeführerin wurde vom VwGH schon allein deshalb zugelassen, weil das BVwG in unrichtiger Auslegung von Art. 99 DSGVO iVm §§ 69 f DSG auf einen Sachverhalt, der einen möglicherweise rechtswidrigen, aber in der Vergangenheit vor dem Wirksamwerden der DSGVO liegenden Eingriff in das Grundrecht gemäß § 1 DSG Anfang 2014 betraf, die DSGVO rückwirkend angewendet hatte.

Aufgrund dieses Rechtsirrtums habe es das BVwG unterlassen, die Rechtmäßigkeit der Datenverarbeitung durch das BMI und die Notwendigkeit der ungeschwärzten Übermittlung der Niederschrift anhand der Bestimmungen des DSG 2000 genau zu prüfen. Dadurch habe es das angefochtene Erkenntnis, das aufgehoben wurde, mit Rechtswidrigkeit infolge Verletzung von Verfahrensvorschriften belastet

Beschluss vom 28.4.2021, Ra 2019/04/0138

Der VwGH hat eine ao. Amtsrevision der DSB zurückgewiesen. Anlass war ein Beschwerdeverfahren, in dem die Beschwerdeführerin eine Beschwerde wegen Verletzung im Auskunftsrecht gegen die Obfrau eines Vereins persönlich als Beschwerdegegnerin, ohne Hinweis auf deren Organfunktion, statt gegen den Verein gerichtet hatte. Die DSB hatte diese Beschwerde abgewiesen, da die Obfrau nicht als datenschutzrechtlich Verantwortliche in Frage komme. Das BVwG wiederum hatte die entsprechende Eingabe parteienfreundlich so verstanden, dass die Beschwerdeführerin den Zusatz „als Obfrau des Vereins“ nur vergessen habe. Daher wurde der Bescheid aufgehoben und die Sache gemäß § 28 Abs. 3 VwGVG an die DSB zurückverwiesen. Der VwGH erachtete dies als eine in vertretbarer Weise vorgenommene fallbezogene Auslegung einer Parteierklärung, die nicht zum Gegenstand einer Revision gemacht werden kann.

Beschluss vom 26.7.2021, Ra 2018/04/0183

Der VwGH hat eine ao. Amtsrevision der DSB zurückgewiesen. Anlass war ein Beschwerdeverfahren, in dem die DSB im Jahr 2017 eine Beschwerde, noch gestützt auf § 31 Abs. 3 DSG 2000, wegen Zweideutigkeit einer Parteierklärung zurückgewiesen hatte. Das BVwG hatte diesen Bescheid aufgehoben (Erkenntnis vom 21.9.2018, W211 2163944-1), da es sich nicht um einen zweideutigen Antrag, sondern um einen Antrag mit zulässigem Eventualantrag gehandelt habe.

Der VwGH hat dazu festgehalten, dass ein Verbesserungsauftrag nach § 13 Abs. 3 AVG immer nur dann gesetzmäßig ist, wenn der angenommene Mangel tatsächlich vorliegt. Wurde zu Unrecht die Mangelhaftigkeit des Anbringens angenommen (und wäre in der Sache zu entscheiden gewesen), ist die deshalb ergangene zurückweisende Entscheidung unabhängig davon inhaltlich rechtswidrig, ob der Einschreiter nur eine teilweise oder nur eine verspätete „Verbesserung“ vornimmt oder diese gar nicht versucht. Der Verwaltungsgerichtshof hat weiters, auch unter ausdrücklicher Bezugnahme auf § 24 Abs. 2 DSG, festgehalten, dass dem AVG (und damit auch den begleitenden datenschutzrechtlichen Verfahrensbestimmungen) „jeglicher Formalismus fremd“ ist.

Erkenntnis vom 9.8.2021, Ra 2019/04/0106

Diesem Rechtsstreit lag ein Vorfall aus dem Jahr 2015 zugrunde, als das Landesverwaltungsgericht Salzburg (LVwG Sbg) mehrere Monate lang eine Entscheidung, die das Geburtsdatum einer betroffenen Person enthielt (in der Geschäftszahl einer Behörde, siehe auch die folgende Entscheidung des VwGH), auf seiner Website veröffentlicht hatte. Die Datenschutzbehörde (Teilbescheid vom 6.9.2016, GZ: DSB-D122.454/0010-DSB/2016) und das Bundesverwaltungsgericht (Erkenntnis vom 10.7.2019, W101 2140606-1) sahen hier einen unzulässigen Eingriff in das Datenschutzgrundrecht der betroffenen Person durch einen **Akt der Justizverwaltung**.

Der Verwaltungsgerichtshof (VwGH) hat nunmehr der ao. Amtsrevision des LVwG Sbg Folge gegeben und den Spruch der DSB auf Zurückweisung der Beschwerde wegen Unzuständigkeit abgeändert. Der VwGH kommt zu dem Schluss, dass die **Pseudonymisierung** von Entscheidungstexten für Zwecke der Veröffentlichung eine **Aufgabe jener Richter** (Einzelrichter oder Senat) ist, die die jeweilige Entscheidung getroffen haben. Diese Pseudonymisierung ist daher eine **Angelegenheit der Gerichtsbarkeit** und als solche der Zuständigkeit der DSB entzogen. Hinzuweisen ist, dass der VwGH auf diesen Sachverhalt materiellrechtlich noch das DSG 2000 anzuwenden hatte.

Beschluss vom 2.9.2021, Ra 2019/04/0108

Der VwGH hat eine ao. Amtsrevision der DSB zurückgewiesen. Anlass war ein Beschwerdeverfahren, in dem der Beschwerdeführer die Verwendung seines Geburtsdatums zur Bildung eines Verfahrenskennzeichens für Zwecke von Mindestsicherungs-/Sozialhilfeverfahren einer Verwaltungsbehörde im Land Salzburg als Eingriff in sein Geheimhaltungsrecht gerügt hatte. Die DSB hatte der Beschwerde Folge gegeben und einen entsprechenden Eingriff festgestellt (Teilbescheid vom 28.7.2016, GZ: DSB-D122.454/0006-DSB/2016), das BVwG (Erkenntnis vom 16.7.2019, W101 2135622-1) hatte die Beschwerde nach einem Rechtsmittel der Verwaltungsbehörde abgewiesen. Der VwGH hielt in seiner Entscheidung über die Revision neuerlich fest, dass maßgebliche Rechtslage bei Verletzung des Geheimhaltungsrechts jene im Zeitpunkt des Eingriffs ist (das BVwG hatte die DSGVO rückwirkend angewendet). Allerdings ist es der DSB laut VwGH dennoch nicht gelungen, einen relevanten Rechtsirrtum des BVwG aufzuzeigen, da sich die maßgebliche Rechtslage, insbesondere § 1 DSG (2000), nicht geändert habe. Das Sbg MSG (nunmehr: Sozialunterstützungsgesetz – SUG) habe im relevanten Zeitpunkt die Behörden bereits zur Verarbeitung des Geburtsdatums von Antragstellern ermächtigt und war damit aus-

reichende Grundlage für die **Bildung eines Verfahrenskennzeichens unter Einschluss des Geburtsdatums**. Die Datenverarbeitung war damit **zulässig**. Argumente der DSB betreffend die für den angestrebten Zweck (verwechslungssichere Kennzeichnung des Antragstellers) mögliche Verwendung des bPK gemäß E-GovG würden kein gelinderes Mittel im datenschutzrechtlichen Sinn aufzeigen.

Beschluss vom 7.9.2021, Ra 2020/11/0213

In diesem Verfahren betreffend die Zulassung einer ao. Revision in einer fährerscheinrechtlichen Sache hatte der Revisionswerber u.a. vorgebracht, der Führerscheinbehörde nie eine Einwilligung in die Verarbeitung seiner Gesundheitsdaten (betreffend den dem Revisionswerber auferlegten Nachweis des Nichtkonsums von Suchtmitteln) erteilt zu haben. Die entsprechende Datenverarbeitung sei daher mangels einer DSGVO-konformen Rechtsgrundlage unzulässig.

Der VwGH hat dazu unter Hinweis auf vorliegende Rechtsprechung des EuGH festgehalten, dass die Verarbeitung personenbezogener Daten auch ohne Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO erfolgen kann, wenn (lit. e leg. cit.) die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt (vgl. ebenso die Ausnahme des Art. 9 Abs. 2 lit. g DSGVO betreffend u.a. Gesundheitsdaten). Dies sei hier im Interesse der Straßenverkehrssicherheit der Fall, die Revision zeige daher diesbezüglich keine neue Rechtsfrage auf.

Erkenntnis vom 21.10.2021, Ra 2021/04/0119 (und Beschluss vom 27.07.2021, Zuerkennung der aufschiebenden Wirkung)

Das Beschwerdeverfahren (Verfahrenszahl DSB-D122.882) betraf die Frage nach der Berechtigung eines Löschantrags und als logisch vorgeschaltete Voraussetzung die Frage der Zulässigkeit der Verarbeitung von DNA-Daten für erkennungsdienstliche Zwecke durch eine Sicherheitsbehörde. Der Beschwerdeführer war aus Anlass von kriminalpolizeilichen Ermittlungen wegen des Verdachts einer schweren Körperverletzung (§ 84 Abs. 4 StGB, Strafraumen: 6 Monate bis fünf Jahre Freiheitsstrafe) erkennungsdienstlich behandelt, vor Gericht aber wegen Putativnotwehr (Rechtsirrtum über Vorliegen einer Notwehrsituation) freigesprochen worden. Die DSB hatte einer Löschantragbeschwerde hinsichtlich der DNA-Daten Folge gegeben, diese Entscheidung wurde im verwaltungsgerichtlichen Verfahren durch Erkenntnis des BVwG vom 20.4.2021, W214 2223462-1, bestätigt. Die DSB wie das BVwG hatten § 67 Abs. 1 SPG so ausgelegt, dass die Wortfolge „eine mit mindestens einjähriger Freiheitsstrafe bedrohte vorsätzliche gerichtlich strafbare Handlung“ eine Straftat meint, für die das Gesetz eine **Mindeststrafe** in dieser Höhe vorsieht.

Der VwGH hat nunmehr der ao. Amtsrevision des Bundesministers für Inneres Folge gegeben und die entsprechende Bestimmung des SPG verbindlich so ausgelegt, dass jeder Verdacht einer Straftat, für die eine einjährige Freiheitsstrafe, auch wenn es sich dabei um die Höchststrafe handeln sollte, verhängt werden kann, Anlass für die Verarbeitung von DNA-Daten geben kann. Das Erkenntnis des BVwG wurde wegen Rechtswidrigkeit des Inhalts aufgehoben.

Erkenntnis vom 12.11.2021, Ra 2019/04/0055

Dieses Erkenntnis knüpft an den Bescheid der DSB in einem amtswegigen Prüfverfahren (bzw. die abweisende Beschwerdevorentscheidung) vom 8.8.2018, GZ: DSB-D213.658/0002-DSB/2018, sowie an das Erkenntnis des BVwG vom 4.4.2019, W214 2207491-1, an. Gegen letzteres hatte die DSB eine ao. Amtsrevision eingebracht. Streitpunkt war die Frage der Gültigkeit der Einwilligung von Arbeitnehmern in die GPS-Überwachung der von ihnen benutzten Dienstfahrzeuge (GPS-Tracker, Verarbeitung von Bewegungsdaten). Die DSB hatte diesbezüglich durch Bescheid festgestellt, dass Einwilligungserklärungen im Arbeitsverhältnis hier ungültig waren, und angeordnet, die Datenverarbeitung in Einklang mit der DSGVO zu bringen

(z.B. den GPS-Tracker nicht mehr zu verwenden oder eine andere Rechtsgrundlage zu wählen). Die Verantwortliche, eine Gesellschaft.m.b.H., hatte sich ausschließlich auf die Einwilligung berufen und in ihrer Datenschutzerklärung gegenüber ihrer Belegschaft nur die Einwilligung als Rechtsgrundlage angeführt.

Das BVwG hatte den Bescheid der DSB mit der Begründung ersatzlos behoben, dass die DSB alle anderen Rechtsgrundlagen gemäß Art. 6 Abs. 1 DSGVO zu überprüfen habe und nicht nur die Einwilligung. Weiters habe die DSB den Prüfumfang zu eng gefasst.

Der VwGH hat nun festgehalten, dass der DSB **keine Feststellungskompetenz im amtswegigen Prüfverfahren** zukommt. Die **Ausübung der Abhilfebefugnisse setzt keinen separaten Abspruch über die Berechtigung des durchgeführten amtswegigen Prüfverfahrens** voraus. Die Feststellung, dass ein Verstoß gegen die DSGVO vorliegt, ist zwar eine Voraussetzung für die Ausübung der Abhilfebefugnisse, allerdings ist darüber nicht gesondert abzusprechen. Das **Ergebnis von amtswegigen Prüfverfahren** kann daher nur die **Inanspruchnahme der Abhilfebefugnisse gemäß Art. 58 Abs. 2 DSGVO** sein. Sofern der Verstoß inzwischen beseitigt wurde, kommt nur die Einleitung eines Verwaltungsstrafverfahrens in Betracht, um vergangenes Fehlverhalten aufzuzeigen und zu sanktionieren.

Gemäß VwGH ist **Sache** des Bescheids nicht (nur) die Frage der Einwilligung, sondern die **Rechtmäßigkeit der Datenverarbeitung an sich** (also der Einsatz des GPS-Tracker). Der Umstand, dass die DSB sich nur mit der Rechtmäßigkeit gemäß Art. 6 Abs. 1 lit. a DSGVO befasst hat, schadet nicht. Sofern das BVwG die Auffassung vertritt, dass andere Rechtsgrundlagen bzw. ein Wechsel auf andere Rechtsgrundlagen in Betracht kommen, hätte es diese prüfen können. Die ersatzlose Behebung des Bescheids erfolgte daher nicht rechtmäßig.

Beschluss vom 14.12.2021, Ro 2021/04/0006

In der zugrunde liegenden Beschwerdesache (Verfahrenszahl DSB-D124.522) hatte die DSB ihre Zuständigkeit auf Grundlage der DSGVO für Beschwerden gegen Handlungen eines parlamentarischen Untersuchungsausschusses des Nationalrats (BVT-Untersuchungsausschuss, Nennung des Namens eines verdeckten Ermittlers) verneint, das BVwG hatte den entsprechenden Zurückweisungsbescheid jedoch mit dem Argument aufgehoben, dass die DSGVO keine Unterscheidung zwischen den Staatsgewalten Gesetzgebung und Verwaltung treffe (Erkenntnis vom 23.11.2020, W211 2227144-1).

Nach einer Amtsrevision der DSB hat der VwGH nunmehr dem EuGH folgende Auslegungsfragen zur Vorabentscheidung vorgelegt:

1. *Fallen Tätigkeiten eines von einem Parlament eines Mitgliedstaats in Ausübung seines Kontrollrechts der Vollziehung eingesetzten Untersuchungsausschusses unabhängig vom Untersuchungsgegenstand in den Anwendungsbereich des Unionsrechts im Sinne des Art. 16 Abs. 2 erster Satz AEUV, sodass die 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 - DSGVO) auf die Verarbeitung personenbezogener Daten durch einen parlamentarischen Untersuchungsausschuss eines Mitgliedstaates anwendbar ist?*

Falls Frage 1 bejaht wird:

2. *Fallen Tätigkeiten eines von einem Parlament eines Mitgliedstaats in Ausübung seines Kontrollrechts der Vollziehung eingesetzten Untersuchungsausschusses, der Tätigkeiten einer polizeilichen Staatsschutzbehörde, somit den Schutz der nationalen Sicherheit betreffende Tätigkeiten im Sinne des 16. Erwägungsgrundes der Datenschutz-Grundverordnung zum Untersuchungsgegenstand hat, unter den Ausnahmetatbestand des Art. 2 Abs. 2 Buchst. a DSGVO?*

Falls Frage 2 verneint wird:

3. *Sofern - wie vorliegend - ein Mitgliedstaat bloß eine einzige Aufsichtsbehörde nach Art. 51 Abs. 1 DSGVO errichtet hat, ergibt sich deren Zuständigkeit für Beschwerden im Sinne des Art. 77 Abs. 1 in Verbindung mit Art. 55 Abs. 1 DSGVO bereits unmittelbar aus der Datenschutz-Grundverordnung?*

Erkenntnis vom 14.12.2021, Ro 2021/04/0007

In diesem Erkenntnis hat der VwGH (mit ausführlicher Begründung) eine wohl endgültige Entscheidung betreffend die Qualität der statistisch und soziodemografisch errechneten Marketingklassifikationen zur „Parteiaffinität“ als personenbezogene Daten getroffen. Grundlage war der in einem amtswegigen Prüfverfahren ergangene Bescheid der DSB vom 11.2.2019 (Verfahrenszahl: DSB-D213.747). Sowohl die DSB wie das BVwG (Erkenntnis vom 26.11.2020, W258 2217446-1) hatten in ihren Entscheidungen die Frage bejaht, dass die Verarbeitung eines derartigen Datums den Regeln der DSGVO unterliegt, die Revisionswerberin, ein Post-, Logistik- und Direktmarketingunternehmen, hatte dies bestritten.

Der VwGH hält dazu fest:

„Die den Betroffenen zugeordneten „Parteiaffinitäten“ enthalten jeweils eine Wahrscheinlichkeitsaussage über die Neigungen dieser Personen, die im Rahmen der verfahrensgegenständlichen Verarbeitung unstrittig namentlich bezeichnet und damit zweifelsfrei identifiziert im Sinne des Art. 4 Z 1 DSGVO waren. Im Sinne der dargestellten Rechtslage sind die verfahrensgegenständlichen Angaben über die Betroffenen als personenbezogene Daten im Sinne des Art. 4 Z 1 DSGVO anzusehen, handelt es sich doch um konkret bezeichneten Personen zugeordnete Aussagen und damit Informationen „über“ diese Personen. Ob diese Einschätzungen zutreffend sind, ist dabei [...] unerheblich. An diesem Ergebnis kann der Umstand nichts ändern, dass die betreffenden Informationen im Wege der Auswertung von Statistiken bzw. Meinungsumfragen aggregiert wurden.“

Diese Auslegung stelle einen „*acte-clair*“ dar, der keiner weiteren Befassung des EuGH bedürfe, da sie auch im Einklang mit vorliegender (und weiter anwendbarer) Rechtsprechung dieses Gerichtshofs stehe. Es liege weiters jüngste Rechtsprechung des OGH vor, die diese Ansicht ebenfalls bestätige. Daten zu „Parteiaffinitäten“ sind nach Ansicht des VwGH (wie des OGH) auch besonders geschützte (sensible) Daten gemäß Art. 9 Abs. 1 DSGVO.

Der Revision blieb daher der Erfolg versagt, sodass laut Erkenntnis des BVwG rechtskräftig feststeht, dass die Revisionswerberin die Verarbeitung von Daten zur „Parteiaffinität“ für Direktmarketingzwecke zu unterlassen hat.

Erkenntnis des VwGH vom 14.12.2021, Ro 2020/04/0032

Dieses Erkenntnis betrifft einen anderen Teil des zuletzt zitierten Bescheids der DSB. Diesem zufolge hätte die Revisionswerberin gegen ihre Pflicht zur (rechtzeitigen) Durchführung einer Datenschutz-Folgenabschätzung verstoßen, die entsprechende Datenschutz-Folgenabschät-

zung und das Verzeichnis zur Verarbeitungstätigkeit seien fehlerhaft gewesen, und es war angeordnet worden, diese Mängel zu beseitigen.

Das BVwG (Erkenntnis vom 20.8.2020, W258 2217446-1) hatte diesen Bescheid (bis auf die Feststellung betreffend nicht rechtzeitige Durchführung einer Datenschutz-Folgenabschätzung) bestätigt.

Der VwGH hat der Revision nunmehr Folge gegeben und dabei seine weiter oben (Erkenntnis vom 12.11.2021, Ra 2019/04/0055) dargestellte Rechtsprechung zur fehlenden Feststellungskompetenz der DSB zur Anwendung gebracht. Das Erkenntnis des BVwG wurde aufgehoben

4.4 Europäischer Gerichtshof für Menschenrechte

Urteil vom 25.5.2021, Centrum för rättsvisa gegen Schweden (Appl. 35252/08)

In diesem von einer schwedischen NGO angestregten Verfahren ist nun auch die große Kammer des EGMR (siehe Datenschutzbericht 2018, Seite 58) zu dem Schluss gekommen, dass nach einer Gesamtschätzung und unter Berücksichtigung des Ermessensspielraums, den die schwedischen Behörden beim Schutz der nationalen Sicherheit genießen, das schwedische System der signalerkennenden Aufklärung („*bulk interception*“) keine Verletzung von Art. 8 EMRK begründet, jedoch das nationale Rechtssystem gegen derartige Eingriffe mangelhaft ausgestaltet ist bzw. war.

Urteil vom 25.5.2021, Big Brother Watch und andere gegen Vereinigtes Königreich (Appl. 58170/13, 62322/14 und 24960/15)

Auch in dieser Sache ist ein inhaltlich ähnlich gelagertes Urteil der großen Kammer ergangen.

Urteil vom 7.12.2021, Standard Verlagsgesellschaft m.b.H. gegen Österreich (Appl. 39378/15)

Diese Entscheidung (Verletzung von Art. 10 EMRK durch ein Urteil des OGH) betreffend die Pflicht zur Herausgabe der Daten von pseudonymen Nutzern und Kommentatoren im Onlineforum eines Medienunternehmens betrifft das Grundrecht auf Datenschutz insoweit, als der EGMR festhielt, das Verbergen von Identitäten sei ein geeignetes Mittel um den freien Fluss von Meinungen, Ideen und Informationen zu fördern, insbesondere auch im Internet. Medienunternehmen müsse es daher möglich sein, die Identität ihrer Nutzer wirksam zu verteidigen, wenn sich diese zwar einer herabwürdigenden Ausdrucksweise bedienen würden, ihnen aber kein „*Wertungsexzess*“ zur Last falle.

4.5 Europäischer Gerichtshof

EuGH, Urteil vom 15.6.2021, C-645/19

In diesem von einem belgischen Berufungsgericht vorgelegten Vorabentscheidungsverfahren hat der EuGH die Voraussetzungen festgelegt, unter denen eine nationale Aufsichtsbehörde, die hinsichtlich einer grenzüberschreitenden Verarbeitung nicht als federführende Behörde fungiert, ihre Befugnis auszuüben hat, Verstöße gegen die DSGVO einem Gericht ihres Mitgliedsstaats zur Kenntnis zu bringen und gerichtliche Verfahren anhängig zu machen.

Erstens muss die einschreitende Aufsichtsbehörde zum einen abstrakt zu einer solchen Amtshandlung zuständig sein, zum anderen müssen die Bestimmungen der DSGVO betreffend das Verfahren der Zusammenarbeit und Kohärenz beachtet werden. Der EuGH hat klargestellt, dass es mit den Art. 7, 8 und 47 GRC in Einklang steht, dass eine Aufsichtsbehörde eines Mitgliedstaats, die in Bezug auf eine grenzüberschreitende Datenverarbeitung nicht die federführende Aufsichtsbehörde ist, von der Befugnis zur Geltendmachung eines vermeintlichen Verstoßes gegen die DSGVO vor einem Gericht dieses Staates unter Beachtung der Regeln über die Verteilung der Entscheidungsbefugnisse zwischen der federführenden Aufsichtsbehörde und den anderen Aufsichtsbehörden Gebrauch machen kann. Dies allerdings nur in Konstellationen, in denen diese Aufsichtsbehörde zur alleinigen Entscheidung zuständig ist.

Zweitens hat der Gerichtshof entschieden, dass im Fall einer grenzüberschreitenden Datenverarbeitung die Ausübung der Befugnis zur Klageerhebung, die einer Aufsichtsbehörde eines Mitgliedstaats zusteht, die nicht die federführende Aufsichtsbehörde ist, nicht voraussetzt, dass der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter, auf den sich diese Klage bezieht, über eine Hauptniederlassung oder eine andere Niederlassung im Hoheitsgebiet dieses Mitgliedstaats verfügt. Der Verantwortliche oder der Auftragsverarbeiter muss lediglich irgendwo im Gebiet der Europäischen Union über eine Niederlassung verfügen.

Drittens hat der EuGH entschieden, dass im Fall eines solchen Verfahrens die Befugnis einer Aufsichtsbehörde eines Mitgliedstaats, die nicht die federführende Aufsichtsbehörde ist, sowohl in Bezug auf die Hauptniederlassung des für die Verarbeitung Verantwortlichen, die sich in dem Mitgliedstaat, dem diese Behörde angehört, befindet, als auch gegenüber einer anderen Niederlassung dieses Verantwortlichen ausgeübt werden kann. Voraussetzung ist lediglich, dass die DSGVO gilt.

Viertens hat der Gerichtshof entschieden, dass derartige Verfahren, die im zeitlichen Anwendungsbereich der Richtlinie 95/46/EG eingeleitet worden sind, auch im zeitlichen Anwendungsbereich der DSGVO und gestützt auf letztere fortgesetzt werden können.

Fünftens hat der EuGH die unmittelbare Wirkung von Art. 58 Abs. 5 DSGVO betont, wonach dieser auch dann anwendbar sei, wenn er in der Rechtsordnung eines Mitgliedstaats nicht speziell umgesetzt worden ist.

EuGH, Urteil vom 22.6.2021, C-439/19

In diesem vom lettischen Verfassungsgerichtshof initiierten Vorabentscheidungsverfahren hatte sich der EuGH u.a. mit der Abgrenzung zwischen DSGVO und DSRL-PJ zu befassen. Gegenstand war die Frage der Zulässigkeit der Verarbeitung (Veröffentlichung) von Daten zu Strafpunkten wegen Verkehrsübertretungen.

Der EuGH stellt erstens fest, dass eine solche eine „*Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten*“ gemäß Art. 10 DSGVO darstellt, für die die DSGVO wegen der besonderen Sensibilität der betreffenden Daten einen erhöhten Schutz vorsieht.

In diesem Zusammenhang führt der Gerichtshof einleitend aus, dass die Informationen über Strafpunkte personenbezogene Daten darstellen und dass ihre Übermittlung durch die lettische Direktion für Verkehrssicherheit an Dritte eine Verarbeitung darstellt, die in den sachlichen Anwendungsbereich der DSGVO fällt. Dieser Anwendungsbereich sei „*sehr weit*“ gefasst zu verstehen. Die entsprechende Verarbeitung fällt demnach zum einen nicht unter die Ausnahme, wonach die DSGVO keine Anwendung auf eine Verarbeitung im Rahmen einer Tätigkeit findet, die nicht in den Anwendungsbereich des Unionsrechts fällt. Diese Ausnahme ist so zu verste-

hen, dass damit vom Anwendungsbereich der DSGVO allein Verarbeitungen personenbezogener Daten ausgenommen werden sollen, die von staatlichen Stellen im Rahmen einer Tätigkeit, die der Wahrung der nationalen Sicherheit dient, oder einer Tätigkeit, die derselben Kategorie zugeordnet werden kann, vorgenommen werden. Dazu zähle die Straßenverkehrssicherheit nicht. Zum anderen ist die Übermittlung personenbezogener Daten über Strafpunkte auch keine Verarbeitung, die von der Ausnahme erfasst wird, wonach die DSGVO auf Verarbeitungen personenbezogener Daten durch die zuständigen Behörden im Bereich des Strafrechts keine Anwendung findet. Bei der Direktion für Verkehrssicherheit handle es sich nämlich nicht um die „zuständige Behörde“ (dies wäre jene, die das Verfahren geführt und die Strafe verhängt hat).

Bei Entscheidung der Frage, ob eine Verarbeitung von Daten betreffend „Straftaten“ vorliege, für die ein verstärkter Schutz gilt, stellte der EuGH fest, dass es sich um einen autonomen Begriff des Unionsrechts handelt, der in der gesamten Union autonom und einheitlich auszulegen ist. Nach einem Hinweis auf die drei Kriterien, die für die Beurteilung des strafrechtlichen Charakters einer Zuwiderhandlung maßgeblich sind, nämlich die rechtliche Einordnung der Zuwiderhandlung im innerstaatlichen Recht, die Art der Zuwiderhandlung und der Schweregrad der drohenden Sanktion, führte der Gerichtshof aus, dass die fraglichen Verkehrsverstöße unter den Begriff „Straftaten“ im Sinne der DSGVO fallen. Zweitens entschied der Gerichtshof, dass die DSGVO der lettischen Regelung entgegensteht, die die Direktion für Verkehrssicherheit verpflichtet, die Daten über Strafpunkte der Öffentlichkeit zugänglich zu machen. Der EuGH hat in diesem Zusammenhang jedoch hervorgehoben, dass das mit der lettischen Regelung verfolgte Ziel der Verbesserung der Straßenverkehrssicherheit ein von der Union anerkanntes Ziel im allgemeinen Interesse darstellt und dass die Mitgliedstaaten somit die Straßenverkehrssicherheit als „Aufgabe ..., die im öffentlichen Interesse liegt“ einstufen können. Allerdings ist nicht nachgewiesen, dass die lettische Regelung der Übermittlung personenbezogener Daten über Strafpunkte zur Gewährleistung des verfolgten Ziels erforderlich ist.

Drittens entschied der EuGH, dass die DSGVO der lettischen Regelung auch insoweit entgegensteht, als sie es der Direktion für Verkehrssicherheit erlaubt, Daten über Strafpunkte, die gegen Fahrzeugführer wegen Verkehrsverstößen verhängt wurden, an Wirtschaftsteilnehmer zu übermitteln, damit diese sie weiterverwenden und an die Öffentlichkeit übermitteln können.

EuGH, Urteil vom 25.11.2021, C-102/20

Ausgangsverfahren war ein UWG-Rechtsstreit zwischen zwei deutschen Energieversorgungsunternehmen über die wettbewerbsrechtliche Zulässigkeit von sogenanntem „Inbox-Advertising“, bei dem einer Nutzerin/einem Nutzer eines kostenlosen E-Maildienstes in das Eingangsverzeichnis ihrer/seiner Mailbox gekennzeichnete, aber sonst wie E-Mails in Erscheinung tretende Werbenachrichten eingeblendet werden. Der deutsche BGH hat dem EuGH dazu unter anderem Fragen zur Auslegung von Art. 2 lit. h und Art. 13 Abs. 1 der Richtlinie 2002/58/EG (E-Privacy-Richtlinie) vorgelegt.

Den Schlussanträgen des Generalanwalts folgend hat der EuGH insbesondere festgehalten, dass die **Begriffe „elektronische Post“ und damit zusammenhängende Direktwerbung** teleologisch **weit** (über den Wortlaut des Art. 2 lit. h der Richtlinie 2002/58/EG hinaus, wo ausdrücklich nur eine „über ein öffentliches Kommunikationsnetz **verschickte** Text-, Sprach-, Ton- oder Bildnachricht“ als elektronische Post definiert ist) und losgelöst von bestimmten existenten technischen Prozessen oder Applikationen (etwa „klassischer E-Mail“) **auszulegen** sind. Daher fällt „Inbox-Advertising“ unter die Verwendung elektronischer Post für Zwecke der Direktwerbung. Der EuGH geht daher von einer **Pflicht** des Verantwortlichen aus, eine **Einwilligung** der

betroffenen Person (Inhaber/in der Mailbox) **einzuholen**; ob dies im Anlassfall erfolgt ist, sei von den nationalen Gerichten zu prüfen.

In diesem Sinne ist die Entscheidung (laut ausdrücklicher Aussage des EuGH) auch für die Auslegung der entsprechenden Begriffe im zeitlichen Anwendungsbereich der DSGVO von Bedeutung.

EuGH (GA), Schlussanträge vom 2.12.2021, C-319/20

Der Rechtssache liegt ein Vorabentscheidungsersuchen des deutschen BGH zur Auslegung von Art. 80 Abs. 2 DSGVO zugrunde. Angelpunkt ist die Frage, ob ein Verbraucherschutzverband, der sich (unter anderem) mit der Vertretung von Datenschutzinteressen befasst, befugt ist, **ohne Darstellung eines individuellen Betroffenenfalles** eine neben dem Datenschutzrecht auch auf Wettbewerbs- und Verbraucherschutzrecht gestützte Klage mit dem Ziel der objektiven Rechtskontrolle, zu der ihn das deutsche Verfahrensrecht ermächtigt, einzubringen, oder ob der letzte Halbsatz von Art. 80 Abs. 2 DSGVO („*wenn ihres Erachtens die Rechte einer betroffenen Person gemäß dieser Verordnung infolge einer Verarbeitung verletzt worden sind*“) bedingt, dass für datenschutzrechtliche Aspekte einer solchen Klage eine individuelle Beschwerde darzustellen ist. Hintergrund ist die Frage der Gültigkeit einer Facebook Ireland Ltd. erteilten Einwilligung bei der Datenverarbeitung für Online-Dienste.

Generalanwalt *de la Tour* kommt dabei in teleologischer Interpretation der Bestimmung zu dem Schluss, dass es **nicht** die **Intention der Gesetzgeber der DSGVO** war, bei Wirksamwerden der DSGVO bestehende **Klagsrechte von Verbraucherschutzverbänden einzuschränken**. Daher sei eine die Klage legitimierende Auslegung von Art. 80 Abs. 2 DSGVO geboten.

5 Datenschutz-Grundverordnung und Datenschutzgesetz – Erfahrungen und legislative Maßnahmen

5.1 Allgemeine Erfahrungen der DSB im Berichtszeitraum, einschließlich Parlamentarischer Anfragen

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 Verfahrenszahlen und Personalstand

Die Verfahrenszahlen pendelten sich im Jahr 2020 auf einem hohen Niveau ein, das aufgrund von Ereignissen Ende 2021 aber deutlich überschritten wurde (Näheres dazu unten).

Der Personalstand der DSB hat sich im Vergleich zum Jahr 2020 erhöht, worauf bereits im Datenschutzbericht 2020 hingewiesen wurde. Konkret stehen der DSB seit 2021 5 zusätzliche Planstellen des höheren Dienstes und 2 zusätzliche Planstellen des gehobenen Dienstes sowie Budgetmittel für 5 Verwaltungspraktikanten, die für jeweils 1 Jahr aufgenommen werden können, zur Verfügung.

Die hohen Verfahrenszahlen der Jahre 2018 und 2019, gepaart mit einem zu niedrigen Personalstand²⁷, führten dazu, dass die in diesem Zeitraum anhängig gemachten Verfahren teilweise noch im Jahr 2021 anhängig waren. Um diese Verfahren sowie jene, die im Jahr 2020 anhängig gemacht wurden (im Summe rund 800), zügig zu beenden, wurde in den Monaten Juli bis Oktober 2021 die Aktion „**DSB 2.0**“ durchgeführt.

Dazu wurden zwei Gruppen von Bediensteten gebildet: Eine Gruppe (Gruppe A) hatte die ausschließliche Aufgabe, die genannten „Altverfahren“ zu beenden. Die andere Gruppe (B) hatte die Aufgabe, die laufenden Verfahren zu führen. Am Ende des Zeitraumes wurden die noch anhängigen Verfahren auf alle Bediensteten gleichmäßig verteilt.

Durch diese Zweiteilung, verbunden mit einer Entlastung der Gruppe A von allen sonstigen Tätigkeiten, war es möglich, innerhalb des genannten Zeitraumes rund 700 Verfahren zu einem Abschluss zu bringen. Das gesetzte Ziel wurde somit weitgehend erreicht und führte im Ergebnis dazu, dass die individuelle Arbeitsbelastung (Anzahl der konkret zu betreuenden Verfahren je Bedienstetem) sank.

27 Der Personalmangel wurde auch im Bericht der Volksanwaltschaft an den Nationalrat und an den Bundesrat für das Jahr 2020 aufgegriffen; siehe dort S. 103.

Es hatte demnach zunächst den Anschein, dass sich die Verfahrenszahlen des Jahres 2021 auf einem hohen, aber zu bewältigenden Ausmaß stabilisierten.

Ab Dezember 2021 kam es zu einer bis dato nicht dagewesenen Beschwerdewelle aufgrund von Informationsschreiben zur Impfung gegen COVID-19 – teilweise verbunden mit der Zuweisung eines konkreten Impftermins –, die von diversen Ämtern der Landesregierung, dem Dachverband der Sozialversicherungsträger, der Österreichischen Gesundheitskasse sowie dem Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz versandt worden waren.

Die Anzahl der bis Ende 2021 eingebrachten Eingaben in diesem Zusammenhang belief sich auf über 3.000 (!) und überstieg innerhalb eines Monats den Beschwerdeanfall des Jahres 2020 beinahe um das Doppelte.

Um dieser Welle Herr zu werden, wurden der DSB vom Bundesministerium für Justiz zusätzliche Budgetmittel für weitere Verwaltungspraktikanten bereitgestellt.

Es ist daher davon auszugehen, dass die Bearbeitung dieser Eingaben darüber hinausgehende personelle Kapazitäten der DSB im Jahr 2022 binden wird, zumal die DSB verpflichtet ist, jede Eingabe in Behandlung zu nehmen.

5.1.2. Vorabentscheidungsersuchen an den EuGH

Das Jahr 2021 war gekennzeichnet von einem sprunghaften Anstieg der an den EuGH gerichteten Vorabentscheidungsverfahren zur Auslegung der DSGVO.

In 27 Fällen – also im Schnitt mehr als zweimal pro Monat – richteten nationale (Höchst) Gerichte Vorabentscheidungsersuchen an den EuGH, darunter in 4 Fällen aus Österreich (C-154/21, C-300/21, C-446/21, jeweils vorgelegt vom OGH, und C-487/21, vorgelegt vom Bundesverwaltungsgericht). Die DSB ist Verfahrenspartei des Verfahrens zu C-487/21.

Diese Zahl belegt, dass nationale (Höchst-)Gerichte vermehrt mit strittigen Auslegungsfragen zur DSGVO befasst sind und den EuGH ersuchen, dazu Stellung zu nehmen.

Beispielsweise geht um die Klärung folgender, wesentlicher Fragen:

- Verhältnis der Rechtsbehelfe nach Art. 77 (Beschwerde an die Aufsichtsbehörde) und Art. 79 (gerichtliche Klage) zueinander: C-132/21
- Umfang des Auskunftsrechts nach Art. 15 DSGVO: C-154/21, C-487/21 und C-579/21
- Rechtsgrundlage der Datenverarbeitung von Facebook: C-252/21 und C-446/21
- Kündigungsschutz von Datenschutzbeauftragten: C-453/21
- Anwendbarkeit der DSGVO auf Datenverarbeitungen im Zuge nationaler Wahlen: C-306/21
- Strafverfahren nach Art. 83 DSGVO gegen juristische Personen, Frage der Notwendigkeit einer Zurechnung des strafbaren Handelns im Wege einer vertretungsbefugten natürlichen Person: C-807/21
- Reichweite des (immateriellen) Schadenersatzes nach Art. 82 DSGVO: C-300/21, C-687/21, C-741/21.

Mit einem Abschluss dieser Verfahren ist im Jahr 2023 zu rechnen.

5.1.3. Beschwerden an die Volksanwaltschaft

In 8 Fällen wurde die Datenschutzbehörde von der Volksanwaltschaft zur Stellungnahme aufgefordert, weil sich Beschwerdeführer an sie gewendet hatten. Ein Großteil dieser Beschwerden betraf die Verfahrensdauer vor der Datenschutzbehörde (im Zusammenhang mit den unter Punkt 5.1.1. beschriebenen Verfahren, die im Sommer 2021 gezielt abgearbeitet wurden). In 2 Fällen wurde der Beschwerde Berechtigung zuerkannt.

5.1.4. Parlamentarische Anfragen

Das Jahr 2021 war auch durch eine – im Vergleich zu den Vorjahren – hohe Anzahl an parlamentarischen Anfragen geprägt, die die Tätigkeit der Datenschutzbehörde betrafen:

- 5472/J „Mangelnder Datenschutz auf [oesterreich-testet.at](https://www.oesterreich-testet.at)“
- 5505/J „Datenschutzkonforme Vormerkung/Anmeldung bei den Corona-Impfplattformen der Länder“
- 6847/J „Datenschutzbehörde – Handhabung Datenspeicherung“
- 7661/J „Datenschutzverstoß Jö Bonusclub“
- 8015/J „Folgeanfrage mangelnder Datenschutz auf [oesterreich-testet.at](https://www.oesterreich-testet.at)“ und
- 8210/J „Datenschutzrechtliche Zulässigkeit des AMS-Projekts Jobimpuls“

Parlamentarische Anfragen, die die Tätigkeit der DSB betreffen, sind von der Bundesministerin für Justiz zu beantworten. Da es sich bei der DSB um eine unabhängige Behörde handelt, sieht § 19 Abs. 3 DSGVO vor, dass die Leiterin der DSB nur insoweit verpflichtet ist, der Bundesministerin für Justiz über Gegenstände der Geschäftsführung Auskunft zu erteilen, als dies nicht der völligen Unabhängigkeit der DSB widerspricht.

In der Praxis werden daher Auskünfte zu individuellen Verfahren nicht erteilt, weil die Verfahrensführung den Kernbereich der unabhängigen Tätigkeit der DSB bildet.

5.1.5. Beschwerden betreffend die so genannte „Islamlandkarte“

Die erneute Onlineschaltung der „Islamlandkarte“ (<https://www.islam-landkarte.at/>) und die damit verbundene Medienberichterstattung hatten zur Folge, dass Mitte des Jahres 2021 bei der Datenschutzbehörde 45 Beschwerden eingebracht wurden. Im Großteil der Beschwerdevorbringen wurde eine Verletzung der Informationspflicht gemäß Art. 13 und 14 DSGVO moniert. Im Leitverfahren wurde darüber hinaus eine Verletzung im Recht auf Geheimhaltung gemäß § 1 Abs. 1 DSGVO wegen Veröffentlichung personenbezogener Daten geltend gemacht und die generelle Zulässigkeit der „Islamlandkarte“ in Frage gestellt.

Die Verfahren wurden im Berichtszeitraum eingeleitet, abschließende bescheidmäßige Erledigungen sind nicht erfolgt.

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

5.2.1. Allgemeine Informationen

COVID-19 bestimmte für die DSB, wie für alle Menschen, den Rhythmus des Jahres 2021.

Im Vergleich zum Jahr 2020, als die Maßnahmen zur Verhinderung der Ausbreitung von COVID-19 alle Menschen überraschend trafen, war 2021 – soweit es möglich war – ein „Gewöhnungseffekt“ zu bemerken.

Von September 2020 bis Juli 2021 wurde Dienst in „Schichten“ versehen: zwei Gruppen verrichteten im Zwei-Wochen-Takt den Dienst von zuhause aus bzw. im Büro, eine Gruppe war permanent vor Ort, eine Gruppe war permanent zuhause. Die letztlich erfolgte Umstellung auf ausschließlich elektronische Aktenführung – dh. das Abgehen von der „dualen Aktenführung“ in digitaler und Papierform – erleichterte diesen Prozess erheblich.

Zwischen Juli 2021 und Dezember 2021 arbeiteten die Bediensteten in der Behörde, mit Beginn des Lockdowns im Dezember 2021 erfolgte wiederum eine Rückkehr zum „Schichtbetrieb“. Die Bereitschaft des BMJ, die Bediensteten der DSB in das Impfprogramm gegen COVID-19 einzubeziehen, ermöglichte es, dass ein Großteil der Bediensteten bis zum Sommer 2021 die Schutzimpfung in den vom BMJ organisierten Impfstraßen erhielt.

Dank der Impfung und auch aufgrund der behördenintern ergriffenen Vorsichtsmaßnahmen konnten Infektionen mit COVID-19 bis auf wenige Ausnahmefälle vermieden werden.

5.2.2. Rechtliche Fragestellungen und Entscheidungen der DSB

Die im März 2020 erstellten und auf der Website der Datenschutzbehörde abrufbaren Informationen zu COVID-19 werden seither laufend aktualisiert und an die jeweilige Gesetzeslage angepasst. Auch Entscheidungen der Datenschutzbehörde werden dabei berücksichtigt.

Die Verfahren des Jahres 2021 drehten sich zu einem gewissen Teil um COVID-19 und die damit im Zusammenhang stehenden Datenverarbeitungen (siehe dazu im Detail Kapitel 3.2.1.1.).

Losgelöst davon nahm die Entwicklung und Einführung des so genannten „Grünen Passes“ sowohl auf europäischer als auch auf österreichischer Ebene personelle Kapazitäten der DSB in Anspruch, weil die Funktionsweise des Grünen Passes ohne die Verarbeitung personenbezogener Daten nicht gegeben ist. Die DSB hat sowohl auf europäischer Ebene (im Rahmen des EDSA) als auch auf österreichischer Ebene federführend an der legislativen Umsetzung mitgewirkt und zahlreiche Stellungnahmen abgegeben bzw. innerhalb des EDSA die Arbeitsgruppe zu diesem Thema geleitet.

Die Vorbereitungen zur Einführung einer allgemeinen Impfpflicht gegen COVID-19 bestimmten gegen Ende des Jahres die Tätigkeit der Datenschutzbehörde.

Zunächst war die Datenschutzbehörde in die Begutachtung des Gesetzesentwurfes eingebunden.

Die beschwerdeintensivste Fragestellung im Berichtszeitraum wurde erst ab Dezember 2021 offenkundig und wird frühestens 2022 entschieden werden: Im Spätherbst 2021 wurden ungeimpfte Personen gezielt von verschiedenen Absendern (Dachverband der Sozialversicherungsträger, Ämter der Landesregierung, ÖGK, Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz) angeschrieben und über die COVID-19- Impfung informiert. Teilweise wurde den Adressaten auch ein Impftermin zugewiesen. Dies hatte die im Vorkapitel beschriebene Beschwerdeflut an die Datenschutzbehörde zur Folge. In diesen Verfahren stellt sich die Frage, ob die jeweiligen Absender befugt waren, die personenbezogenen Daten der Adressaten zu ermitteln und sie in weiterer Folge anzuschreiben.

6 Europäische Zusammenarbeit

6.1 Europäische Union

6.1.1 Der Europäische Datenschutzausschuss

Der Europäische Datenschutzausschuss (EDSA) hat sich im Jahr 2021 15 Mal zu Plenarsitzungen getroffen. Eine dieser Sitzungen fand in Brüssel statt, die restlichen Plenarsitzungen wurden via Videokonferenz abgehalten.

Die im Rahmen dieser Treffen besprochenen Themen und angenommenen Dokumente wurden größtenteils in den 11 Experten-Untergruppen des EDSA vorbereitet, die sich im Jahr 2021 insgesamt 200 Mal fast ausschließlich per Videokonferenz getroffen haben. Eine Auswahl dieser Dokumente wird im Folgenden näher genannt bzw. deren Inhalt dargelegt.

Der EDSA hat im vergangenen Jahr erstmals einen Beschluss im Dringlichkeitsverfahren gemäß Art. 66 Abs. 2 DSGVO (1/2021, 12. Juli 2021)²⁸ angenommen. Dieser erfolgte auf Antrag der Hamburger Aufsichtsbehörde, die in ihren einstweiligen Maßnahmen gemäß Art. 66 Abs. 1 DSGVO Facebook Ireland Limited (Facebook IE) - infolge Änderung der geltenden Nutzungsbedingungen und Datenschutzrichtlinien von WhatsApp Ireland Limited (WhatsApp IE) - für drei Monate die Verarbeitung der Daten von in Deutschland ansässigen Nutzern durch WhatsApp IE untersagte. Der EDSA entschied in seinem Beschluss, dass die Voraussetzungen für den Nachweis eines Verstoßes gegen die DSGVO und die Dringlichkeit, endgültige Maßnahmen zu ergreifen, nicht erfüllt wären, und stellte fest, dass die irische Aufsichtsbehörde keine endgültigen Maßnahmen gegen Facebook IE ergreifen müsse. Allerdings bestünde eine hohe Wahrscheinlichkeit, dass Facebook IE die Nutzerdaten von WhatsApp IE bereits für die gemeinsamen Zwecke verarbeite. Der EDSA sei jedoch nicht in der Lage, mit Sicherheit festzustellen, welche Verarbeitungen tatsächlich durchgeführt würden und in welcher Eigenschaft. Folglich wurde die irische Aufsichtsbehörde aufgefordert, diesbezüglich unverzüglich eine amtswegige Untersuchung durchzuführen.

Zudem wurde ein weiterer verbindlicher Beschluss über den Entwurf einer Entscheidung der irischen Aufsichtsbehörde betreffend WhatsApp IE gemäß Artikel 65 Absatz 1 lit. a DSGVO (1/2021, 28. Juli 2021)²⁹ erlassen. Diesem Streitbeilegungsbeschluss war eine amtswegige Untersuchung durch die irische Aufsichtsbehörde zu den Transparenzverpflichtungen der Verbraucherdienste von WhatsApp IE gegenüber Nutzern und Nicht-Nutzern nach den Artikeln 12, 13 und 14 DSGVO vorangegangen. Der EDSA kam ausgehend von den maßgeblichen und begründeten Einsprüchen gemäß Art. 4 Z 24 DSGVO der anderen Aufsichtsbehörden zu dem Schluss, dass die irische Aufsichtsbehörde ihren Entwurf hinsichtlich einzelner Transparenzverstöße, der Berechnung der Geldbuße und der Frist für die Umsetzung der Anweisung abzuändern habe. Die irische Aufsichtsbehörde hat ihren nationalen Beschluss gemäß Artikel 65 Abs. 6 DSGVO überarbeitet und darin unter anderem die Geldstrafe auf 225 Millionen Euro

28 https://edpb.europa.eu/system/files/2021-07/edpb_urgentbindingdecision_20210712_requesthh_fbireland_en.pdf

29 https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf

erhöht. Der Beschluss des EDSA wird seitens WhatsApp IE mit Klage vor dem Gericht der Europäischen Union vom 1. November 2021 (Rechtssache T-709/21)³⁰ angefochten.

Des Weiteren hat der EDSA gemäß Art. 64 Abs. 1 DSGVO 2020 zu folgenden Themen insgesamt 30 Stellungnahmen³¹ abgegeben:

- 5 Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Überwachung von Verhaltensregeln gemäß Art. 41 DSGVO (Ungarn, Norwegen, Tschechische Republik, Slowakei und Malta);
- 7 Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Zertifizierung gemäß Art. 43 Abs. 3 DSGVO (Portugal, Rumänien, Ungarn, Litauen, Lettland, Belgien und Norwegen);
- eine Stellungnahme zum Entwurf der Standardvertragsklauseln gemäß Art. 28 Abs. 8 DSGVO (Litauen);
- 17 Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (Saxo Bank Group, Elanders Group, 2 Mal zu BDO, 2 Mal zu Kuman Group, 2 Mal Luxoft Group, 2 Mal zu CGI Group, Internet Initiative Japan Group, 2 Mal zu Oregon Tool Inc., 2 Mal zu COLT Group, Carrier und Otis);

Gemäß Art. 64 Abs. 2 DSGVO 2020 hat der EDSA folgende Stellungnahmen³² angenommen:

- zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Verordnung (EU) 2016/679 über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich (14/2021, 13. April 2021) und
- zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Richtlinie (EU) 2016/680 über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich (15/2021, 13. April 2021):

Der EDSA erkannte in beiden Stellungnahmen starke Ähnlichkeiten in den Kernbereichen der Datenschutzgesetze der EU und des Vereinigten Königreichs, betonte aber auch, dass einige Punkte seitens der Europäischen Kommission im Rahmen ihres Beschlusses auf der Grundlage der DSGVO näher bewertet bzw. genau überwacht werden sollten, darunter beispielsweise die Ausnahmeregelung für den Einwanderungsbereich und ihre Auswirkungen auf die für die Rechte der betroffenen Personen geltenden Beschränkungen sowie die Anwendung von Beschränkungen auf Weiterübermittlungen von aus dem EWR stammenden personenbezogenen Daten in das Vereinigte Königreich. Im Hinblick auf den Zugang zu in das Vereinigte Königreich übermittelten personenbezogenen Daten aus Gründen der nationalen Sicherheit hielt der EDSA fest, dass trotz der Befassung eines „Investigatory Powers Tribunal“ und der Einsetzung von „Judicial Commissioners“, das Abfangen von Massendaten, die unabhängige Bewertung und Überwachung des Einsatzes von Instrumenten für die automatisierte Datenverarbeitung sowie im Recht des Vereinigten Königreichs vorgesehene Garantien für Fälle, in denen Daten in Übersee offengelegt werden (insbesondere im Hinblick auf die Anwendung von Ausnahmen aus Gründen der nationalen Sicherheit) präzisiert bzw. überwacht werden sollten.

30 <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021TN0709>.

31 https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de?f%5B0%5D=opinions_date%3A2021&f%5B1%5D=opinions_publication_type%3A61

32 https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de?f%5B0%5D=opinions_date%3A2021&f%5B1%5D=opinions_publication_type%3A60&f%5B2%5D=opinions_publication_type%3A776.

Beim Durchführungsbeschluss gemäß der Richtlinie (EU) 2016/680 handelt es sich um den ersten Entwurf eines solchen Beschlusses zur Angemessenheit eines Rechtssystems eines Drittlandes, den die Europäische Kommission unterbreitet und der EDSA bewertet hat.

- zum Rückverfolgbarkeitssystem für Tabak (20/2021, 18. Juni 2021): In dieser Stellungnahme stimmte der EDSA der Einschätzung der Europäischen Kommission zu, wonach die Mitgliedstaaten und die Kommission als gemeinsam für die Verarbeitung Verantwortliche in Bezug auf die Verarbeitung personenbezogener Daten im Rahmen des EU-Rückverfolgbarkeitssystems für Tabak handelten. Zudem vertrat der EDSA die Auffassung, dass im Falle der gemeinsamen Verantwortlichkeit die bloße Tatsache, dass die ID-Aussteller von dem Mitgliedstaat ernannt werden, nicht unbedingt bedeute, dass diese nur Auftragsverarbeiter des Mitgliedstaates seien. Abschließend stimmte der EDSA mit der Einschätzung der Europäischen Kommission überein, wonach die unabhängigen Dritten, die die primären Datenspeicher hosten, als Sub-Auftragsverarbeiter des Betreibers des sekundären Datenspeichers fungierten, der als Auftragsverarbeiter im Namen der gemeinsam für die Verarbeitung Verantwortlichen (Kommission und Mitgliedstaaten) handelte.
- zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Verordnung (EU) 2016/679 über die Angemessenheit des Schutzes personenbezogener Daten in der Republik Korea (32/2021, 24. September 2021):

In seiner Stellungnahme begrüßte der EDSA die Angleichung des datenschutzrechtlichen Rahmens der EU und Südkoreas in den wesentlichen Schlüsselbereichen, sowie die Bemühungen, durch Annahme von behördlichen Mitteilungen durch die südkoreanische Datenschutzbehörde, wie etwa die Notifizierung Nr. 2021-1, die Lücken zwischen der DSGVO und dem koreanischen Datenschutzrecht zu schließen. Der EDSA ersuchte die Europäische Kommission jedoch um weitere Informationen über den verbindlichen Charakter, die Durchsetzbarkeit und die Gültigkeit der Notifizierung Nr. 2021-1 und empfahl eine aufmerksame Überwachung dieser Aspekte in der Praxis. Hinsichtlich des behördlichen Zugriffs auf in die Republik Südkorea übermittelte personenbezogene Daten ersuchte der EDSA die Europäische Kommission im Hinblick auf wirksame Rechtsbehelfe um Klärung der materiell- bzw. verfahrensrechtlichen Anforderungen – wie beispielsweise solche an die Beweislast –, denen eine Beschwerde bei der südkoreanischen Datenschutzbehörde oder eine Klage vor Gericht unterlägen, und um Klarstellung, ob Personen in der EU eine solche Voraussetzung erfüllen könnten.

- zur Frage, ob Art. 58 Abs. 2 lit. g DSGVO als Rechtsgrundlage dafür dienen kann, dass eine Aufsichtsbehörde von Amts wegen die Löschung personenbezogener Daten anordnet, wenn die betroffene Person keinen entsprechenden Antrag gestellt hat (39/2021, 14. Dezember 2021):

In dieser Stellungnahme kam der EDSA zum Ergebnis, dass Art. 58 Abs. 2 lit. g DSGVO eine geeignete Rechtsgrundlage für die Anweisung der Löschung rechtswidrig verarbeiteter Daten sowohl bei amtswegigen Prüfverfahren (ohne vorheriges Löschbegehren eines Betroffenen), als auch bei Individualbeschwerden wegen eines nicht oder nicht vollständig erfüllten Löschbegehrens durch einen Betroffenen darstelle. Schließlich sei Art. 17 DSGVO, auf den Art. 58 Abs. 2 lit. g referenziert, einerseits als eine Verpflichtung des Verantwortlichen, als auch als Verpflichtung des Tätigwerdens bei einem Löschbegehren des Betroffenen zu interpretieren.

Gemeinsam mit dem Europäischen Datenschutzbeauftragten (EDSB) hat der EDSA folgende Stellungnahmen³³ abgegeben:

- zu Standardvertragsklauseln zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern (1/2021, 14. Jänner 2021):

Diese Standardvertragsklauseln (SVK) haben EU-weite Wirkung und sollen eine vollständige Harmonisierung und Rechtssicherheit bei Vereinbarungen zwischen Verantwortlichen und ihren Auftragsverarbeitern gewährleisten. Aus diesem Grund wurden seitens des EDSB und des EDSA Änderungen im Hinblick auf das Zusammenspiel der beiden Dokumente, auf die sogenannte Koppelungsklausel, die zusätzlichen Stellen einen Rückgriff auf die Standardvertragsklauseln ermöglicht, sowie auf die Pflichten der Auftragsverarbeiter angeregt. Außerdem schlugen der EDSA und der EDSB vor, in den Anhängen der SVK die zwischen den Parteien bestehende Aufgaben- und Rollenverteilung in Bezug auf die einzelnen Verarbeitungstätigkeiten zu präzisieren.

- zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (2/2021, 14. Jänner 2021):

Der Entwurf dieser SVK gemäß Artikel 46 Absatz 2 Buchstabe c DSGVO ersetzt die bestehenden SVK für internationale Datenübermittlungen auf Grundlage der Richtlinie 95/46/EG und soll ferner dem Urteil des EuGH in der Rechtssache „Schrems II“ Rechnung tragen. So stellten der EDSB und der EDSA fest, dass die neuen SVK konkretere Garantien für den Fall, dass die Rechtsvorschriften des Bestimmungslandes die Einhaltung der Klauseln beeinträchtigen (insbesondere bei verbindlichen Ersuchen von Behörden um Offenlegung personenbezogener Daten), enthielten. Beide Institutionen waren aber auch der Auffassung, dass bestimmte Bestimmungen verbessert oder präzisiert werden könnten, etwa betreffend den Anwendungsbereich der SVK, die Rechte von Drittbegünstigten, die Pflichten im Zusammenhang mit der Datenweiterleitung, die Aspekte der Prüfung von in Drittländern geltenden Rechtsvorschriften über den Zugang von Behörden zu öffentlichen Daten sowie die Benachrichtigung der Aufsichtsbehörde.

- zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz) (3/2021, 11. März 2021):

Der EDSB und der EDSA unterstützten in ihrer Stellungnahme das Gesetzesvorhaben, die Bedingungen für die gemeinsame Nutzung von Daten im Binnenmarkt zu verbessern, betonten aber, dass dafür Sorge zu tragen sei, dass das Gesetz in voller Übereinstimmung mit den EU-Rechtsvorschriften zum Schutz personenbezogener Daten stehe und das Niveau des Schutzes personenbezogener Daten von Einzelpersonen weder beeinträchtige noch die in der Datenschutzgesetzgebung festgelegten Rechte und Pflichten ändere. Bezüglich der Gemeinnützigkeit von Daten rieten der EDSB und der EDSA zu einer genaueren Definition dieser Zwecke. Zudem kritisierten die Institutionen, dass die bloßen Meldeverfahren für die Datenweitergabe an Diensteanbieter oder Organisationen kein hinreichend strenges Prüfverfahren für solche Dienste vorsähen. Zudem wurden Empfehlungen für die Benennung der Aufsichtsbehörden als hauptverantwortliche Behörden für die Kontrolle der Einhaltung des Daten-Governance-Gesetzes in Absprache mit anderen sektorspezifischen Behörden ausgesprochen.

- zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ei-

33 https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de?f%5B0%5D=opinions_date%3A2021&f%5B1%5D=opinions_publication_type%3A553.

nen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von Impfungen, Tests und der Genesung mit der Zielsetzung der Erleichterung der Freizügigkeit während der COVID-19-Pandemie (Digitales Grünes Zertifikat) (4/2021, 31. März 2021):

Mit dem digitalen grünen Zertifikat soll ein gemeinsamer Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von Impfungen, Tests und der Genesung im Zusammenhang mit COVID-19 geschaffen und damit die Ausübung des Rechts auf Freizügigkeit innerhalb der EU während der COVID-19-Pandemie erleichtert werden. In ihrer Stellungnahme bestanden der EDSB und der EDSA darauf, dass dabei die Grundsätze der Wirksamkeit, Erforderlichkeit, Verhältnismäßigkeit und Nichtdiskriminierung eingehalten würden. In dem Vorschlag sollten klare und präzise Regeln für den Geltungsbereich und die Anwendung des digitalen grünen Zertifikats Niederschlag finden und geeignete Garantien vorgesehen werden. Zudem müsse ausdrücklich festgehalten werden, dass der Zugriff auf personenbezogene Daten und deren anschließende Nutzung durch die EU-Mitgliedstaaten nach dem Ende der Pandemie nicht mehr gestattet seien. Die gemeinsame Stellungnahme enthält weiters konkrete Empfehlungen betreffend die Präzisierung von betroffenen Datenkategorien, die Datenspeicherung, die Transparenzpflichten und die Identifizierung der für die Verarbeitung personenbezogener Daten Verantwortlichen und Auftragsverarbeiter.

- zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) (5/2021, 18. Juni 2021):

Der EDSB und EDSA begrüßten grundsätzlich den Vorschlag einer solchen Verordnung, bedauerten jedoch, dass die internationale Zusammenarbeit auf dem Gebiet der Strafverfolgung nicht in den Anwendungsbereich des Vorschlags falle. Weiters sei in der Verordnung klarzustellen, dass die bestehenden EU-Rechtsvorschriften zum Datenschutz (DSGVO, EU-DSVO und Richtlinie zum Datenschutz bei der Strafverfolgung) auf jede Verarbeitung personenbezogener Daten anwendbar seien, die in den Anwendungsbereich des Vorschlags für die Verordnung falle. Der risikobasierte Ansatz des Verordnungsentwurfes sei zu begrüßen, doch sei das Konzept der „Risiken für die Grundrechte“ an den EU-Datenschutzrahmen anzupassen und seien die gesellschaftlichen Risiken für Personengruppen ebenfalls zu berücksichtigen und zu mindern. Angesichts der extrem hohen Risiken der biometrischen Fernidentifizierung von Personen im öffentlichen Raum rieten der EDSB und der EDSA zu einem generellen Verbot der Verwendung von künstlicher Intelligenz für die automatisierte Erkennung menschlicher Merkmale im öffentlichen Raum, darunter die Gesichts-, Gang-, Fingerabdruck-, DNA-, Stimm- und Tippverhaltenserkennung sowie die Erkennung anhand anderer biometrischer oder verhaltensbezogener Charakteristika. Parallel dazu empfahlen beide Institutionen ein Verbot von Künstliche Intelligenz-Systemen, die Personen mithilfe von Biometrie aufgrund ihrer ethnischen Zugehörigkeit, ihres Geschlechts, ihrer politischen oder sexuellen Orientierung oder anderer Gründe in Gruppen einteilen, für die ein Diskriminierungsverbot gemäß Art. 21 der Charta der Grundrechte bestehe. Darüber hinaus vertraten der EDSB und der EDSA die Auffassung, dass die Verwendung von künstlicher Intelligenz zu Rückschlüssen auf die Emotionen einer natürlichen Person keinesfalls wünschenswert sei und verboten werden sollte, wobei nur für sehr spezifische Fälle, wie zum Beispiel medizinische Zwecke, Ausnahmen vorgesehen werden sollten. Zudem sollte die Verwendung von künstlicher Intelligenz für die Bewertung des sozialen Verhaltens („Social Scoring“) verboten werden. Der EDSA und der EDSB begrüßen, dass in dem Vorschlag der EDSB als die zuständige Behörde und Marktüberwachungsbehörde für die Aufsicht über die Organe, Einrichtungen und sonstigen Stellen der Union benannt werde, raten jedoch zu

einer Spezifizierung der Aufgaben. Der EDSB und der EDSA sind abschließend der Auffassung, dass die Datenschutzbehörden zur Sicherstellung der reibungslosen Anwendung dieser neuen Verordnung als zuständige nationale Aufsichtsbehörden gemäß Art. 59 des Vorschlags benannt werden sollten.

Zudem hat der EDSA 2020 zu folgenden Themen *Leitlinien*³⁴ verabschiedet:

- zu Beispielen für die Benachrichtigung über Verletzungen des Schutzes personenbezogener Daten (1/2021, 14. Dezember 2021):

Diese Leitlinien ergänzen die WP 29-Leitlinien zur Meldung von Datenschutzverletzungen und bieten eine in Fallgruppen gestaffelte Übersicht über diverse Kategorien von Sicherheitsverletzungen, die von den nationalen Aufsichtsbehörden als am häufigsten wahrgenommen werden, wie z. B. Ransomware-Angriffe, Angriffe zur Datenexfiltration sowie verlorene oder gestohlene Geräte und Dokumente. Es werden jeweils Fälle zu unterschiedlichen Risikoszenarien und damit korrespondierenden, durch den datenschutzrechtlich Verantwortlichen vorzunehmenden Maßnahmen, einschließlich die Benachrichtigung der betroffenen Personen, erläutert.

- zu virtuellen Sprachassistenten (2/2020, 7. Juli 2021):

Diese Leitlinien identifizieren die wichtigsten datenschutzrechtlichen Compliance-Herausforderungen rund um intelligente Sprachassistenten und geben den beteiligten Stakeholdern Empfehlungen, wie diese bewältigt werden können. Insbesondere wurde das diesbezügliche Spannungsverhältnis zwischen der DSGVO und der E-Privacy-Richtlinie (RL 2001/58/EG) näher dargestellt.

- zur Anwendung von Artikel 65 Absatz 1 Buchstabe a der Datenschutz-Grundverordnung (3/2021, in öffentlicher Konsultation):

Diese Leitlinie behandelt den Streitbeilegungsmechanismus gemäß Art. 65 Abs. 1 lit. a DSGVO, wenn die federführende Aufsichtsbehörde sich den maßgeblichen und begründeten Einsprüchen anderer Aufsichtsbehörden gegen ihren Entscheidungsentwurf nicht angeschlossen hat oder diese als nicht maßgeblich oder nicht begründet ablehnt. Dabei werden die wichtigsten Verfahrensschritte dargelegt, die Zuständigkeit des EDSA bei der Annahme einer rechtsverbindlichen Entscheidung auf der Grundlage von Art. 65 Abs. 1 lit. a DSGVO geklärt und die geltenden Verfahrensgarantien und Rechtsbehelfe beschrieben.

- zu Verhaltensregeln als Übermittlungsinstrumente (4/2021, in öffentlicher Konsultation):

Diese Leitlinien ergänzen die Leitlinien 1/2019 über Verhaltensregeln, die einen allgemeinen Rahmen für die Annahme von Verhaltensregeln vorgeben, und sollen die Anwendung von Art. 40 Abs. 3 und Art. 46 Abs. 2 lit. e DSGVO präzisieren. Nach diesen Bestimmungen können sich – nach Genehmigung durch eine zuständige Aufsichtsbehörde und Erklärung ihrer allgemeinen Gültigkeit innerhalb des EWR durch die Kommission – Verantwortliche und Auftragsverarbeiter, die der DSGVO nicht unterliegen, ebenfalls den Verhaltensregeln anschließen und diese anwenden, um geeignete Garantien für Datenübermittlungen außerhalb der EU vorzusehen.

34 Siehe hierzu https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de?f%5B0%5D=opinions_date%3A2021&f%5B1%5D=opinions_publication_type%3A64.

- zum Zusammenspiel zwischen der Anwendung von Artikel 3 und den Bestimmungen über internationale Übermittlungen gemäß Kapitel V der Datenschutz-Grundverordnung (5/2021, in öffentlicher Konsultation):

Diese Leitlinien sollen die Verantwortlichen und Auftragsverarbeiter in der EU dabei unterstützen, festzustellen, ob es sich bei einem Verarbeitungsvorgang um eine internationale Übermittlung handelt. Eine Verarbeitung könne anhand dreier kumulativer Kriterien als Übermittlung eingestuft werden: 1. Der Datenexporteur (ein Verantwortlicher oder Auftragsverarbeiter) unterliegt für die betreffende Verarbeitung der DSGVO; 2. der Datenexporteur übermittelt die personenbezogenen Daten dem Datenimporteur (einem anderen Verantwortlichen, einem gemeinsam Verantwortlichen oder einem Auftragsverarbeiter) oder stellt diese zur Verfügung; 3. der Datenimporteur ist in einem Drittland ansässig oder ist eine internationale Organisation. Die Verarbeitung gelte dabei als Übermittlung, unabhängig davon, ob der in einem Drittland niedergelassene Importeur bereits gemäß Art. 3 DSGVO dieser unterliegt. Der EDSA ist jedoch der Auffassung, dass die Erhebung von Daten direkt von betroffenen Personen in der EU auf eigene Initiative keine Übermittlung darstelle.

Darüber hinaus wurden auch drei *Empfehlungen*³⁵ des EDSA zu folgenden Themen angenommen:

- zu Maßnahmen, die die Übermittlungsinstrumente ergänzen, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten (1/2020, 18. Juni 2021):

Die Empfehlungen wurden erstmals im November 2020 nach dem Urteil des EuGH in der Rechtssache „Schrems II“ (C-311/18) angenommen. Sie zielen darauf ab, Verantwortliche und Auftragsverarbeiter, die als Datenexporteure fungieren, bei der Ermittlung und Durchführung geeigneter zusätzlicher Maßnahmen zu unterstützen, wenn diese erforderlich sind, um ein gleichwertiges Datenschutzniveau für die in Drittstaaten übermittelte Daten zu gewährleisten. Die endgültige Fassung der Empfehlung enthält folgende wichtige Änderungen:

Hervorhebung der Bedeutung einer Prüfung der Praktiken von Behörden in Drittstaaten bei der rechtlichen Bewertung durch die Datenexporteure im Hinblick auf die Beeinträchtigung der Wirksamkeit des Übermittlungsinstruments gemäß Art. 46 DSGVO; die Möglichkeit, dass der Datenexporteur bei seiner Bewertung die praktische Erfahrung des Datenimporteurs berücksichtigt und die Klarstellung, dass die Rechtsvorschriften des Bestimmungsdrittlandes, das seinen Behörden den Zugriff auf die übermittelten Daten auch ohne die Intervention des Datenimporteurs erlauben, die Wirksamkeit des Übermittlungsinstruments beeinträchtigen können.

- zur Referenzgrundlage für den Begriff „Angemessenheit“ in der Richtlinie zum Datenschutz bei der Strafverfolgung (1/2021, 2. Februar 2021):

Ziel der Empfehlungen ist es, eine Liste von Elementen zu erstellen, die bei der Bewertung der Angemessenheit des Datenschutzniveaus eines Drittstaates im Rahmen der Richtlinie (EU) 2016/680 zu prüfen sind. Das Dokument verweist auf das Konzept und die Verfahrensaspekte der Angemessenheit gemäß der Richtlinie (EU) 2016/680 und der Rechtsprechung des EuGH und legt die EU-Standards für den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen fest.

35 https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de?f%5B0%5D=opinions_date%3A2021&f%5B1%5D=opinions_publication_type%3A98.

- zur Rechtsgrundlage für die Speicherung von Kreditkartendaten ausschließlich zum Zweck der Erleichterung weiterer Online-Transaktionen (2/2021, 19. Mai 2021):

Die Empfehlungen beziehen sich auf Situationen, in denen betroffene Personen auf einer Website oder über eine Anwendung ein Produkt kaufen oder eine Dienstleistung bezahlen und dabei im Zuge der Transaktion ihre Kreditkartendaten eingeben. Der EDSA hielt hierzu fest, dass lediglich die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO als geeignete Rechtsgrundlage für die Speicherung von Kreditkartendaten nach Abschluss des Kaufes – etwa zur Erleichterung künftiger Käufe - betrachtet werden könne.

Darüber hinaus haben der EDSA und die einzelnen Aufsichtsbehörden zur *Evaluierung und Überprüfung* der Richtlinie (EU) 2016/680 beigetragen³⁶, die von der Europäischen Kommission durchgeführt wurde. Da die vergangenen vier Jahre vor allem durch die nationalen Prozesse zur Umsetzung der Richtlinie geprägt gewesen seien, gäbe es wenige Erfahrungen und empirische Daten zu einigen Teilen dieser. Es sei nach Ansicht des EDSA daher noch zu früh, um Schlussfolgerungen über die Wirksamkeit der Richtlinie zu ziehen oder ihre Überarbeitung zu erwägen. Der EDSA ersuche die Mitgliedstaaten, die sich noch in der Umsetzungsphase befänden, nachdrücklich, alles in ihrer Macht Stehende zu tun, um sicherzustellen, dass die Umsetzung ohne weitere Verzögerungen vollständig mit der Richtlinie übereinstimme. Der EDSA betonte, dass die wirksame Umsetzung der Aufgaben im Rahmen der Richtlinie die Verfügbarkeit der erforderlichen personellen und technischen Ressourcen erfordere, und forderte die Mitgliedstaaten zur Aufstockung der Ressourcen der Aufsichtsbehörden im Verhältnis zu ihrer Arbeitsbelastung auf.

In Umsetzung der EDSA-Strategie 2021-2023 wurde zudem ein Expertenpool („Support Pool of Experts“ - SPE)³⁷ ins Leben gerufen, um den Mitgliedern des EDSA fachliche Unterstützung zur Verfügung zu stellen, die für Untersuchungen und Durchsetzungsmaßnahmen nützlich ist, und um die Zusammenarbeit und Solidarität zwischen den Mitgliedern des EDSA zu fördern.

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 794/2016³⁸ 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 Europol sowie die Verarbeitung dieser Daten durch den betreffenden Mitgliedstaat zu prüfen. Die Vertreter der nationalen Kontrollbehörden der Mitgliedstaaten und der Europäische Datenschutzbeauftragte bilden gemeinsam den Beirat

36 https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-european-commissions-evaluation-data_en.

37 https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-terms-reference-edpb-support-pool-experts_en.

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

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 der Übermittlung von personenbezogenen Daten an Europol auseinanderzusetzen.

Die österreichische Datenschutzbehörde als nationale Kontrollbehörde überprüfte im Jahr 2021 im Rahmen eines amtswegigen Prüfverfahrens die vom Bundeskriminalamt im Bundesministerium für Inneres als nationale Europol-Stelle durchgeführten Datenübermittlungen an Europol. Das Verfahren konnte positiv abgeschlossen werden.

6.1.3 Schengen

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

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 für das Jahr 2022 erwartet.

Im Dezember 2021 hat die Datenschutzbehörde ein Prüfverfahren betreffend das N.SIS II eingeleitet.

Darüber hinaus haben im Berichtszeitraum Mitarbeiter der Datenschutzbehörde an den Evaluierungen der Länder Griechenland, Italien, Liechtenstein und Niederlande teilgenommen. Die Datenschutzbehörde wird sich auch im Jahr 2022 an Evaluierungen beteiligen.

6.1.4 Zoll

Das gemeinsame Zollinformationssystem (ZIS) dient der Erfassung von Daten von Waren, Transportmitteln, natürlichen und juristischen Personen, die im Zusammenhang mit Verstößen gegen das gemeinsame Zoll- und Agrarrecht stehen. Das ZIS ermöglicht einem Mitgliedstaat, der Daten in das System eingegeben hat, einen ZIS-Partner in einem anderen Mitgliedstaat um die Durchführung u.a. gezielter Kontrollen zu ersuchen. Zur Gewährleistung eines angemessenen Datenschutzes wurde neben dem Ausschuss gemäß Art. 43 der ZIS-Verordnung³⁹ („Joint Supervisory Authority of Customs“ („JSA“)) eine Koordinierende Aufsichtsbehörde (CIS Supervision Coordination Group („CIS-SCG“)) eingerichtet, welche aus Vertretern der nationalen Datenschutzbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten gebildet wird.

39 <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex:31997R0515>.

6.1.5 Eurodac

Das „Eurodac“-System ermöglicht den Einwanderungsbehörden der Mitgliedstaaten Asylwerber und andere Personen zu identifizieren, die beim illegalen Überschreiten einer EU-Außengrenze aufgegriffen werden. Anhand der Fingerabdrücke kann ein Mitgliedstaat feststellen, ob ein Fremder in einem anderen Mitgliedstaat Asyl beantragt hat oder ob ein Asylwerber illegal in die EU eingereist ist. Eurodac besteht aus einer von der Europäischen Kommission verwalteten Zentraleinheit und den in den Mitgliedsstaaten zur Abfrage und Befüllung betriebenen nationalen Systemen. Art. 32 der (EU) Verordnung Nr. 603/2013⁴⁰ sieht eine koordinierte Überwachung durch die nationalen Datenschutzbehörden mit dem Europäischen Datenschutzbeauftragten vor, wobei die Mitgliedstaaten jährlich eine Überprüfung der Verarbeitung personenbezogener Daten durchzuführen haben.

6.1.6 Visa

Das Visa-Informationssystem (VIS) enthält Daten zu Ausstellungen, Ablehnungen, Annullierungen, Widerrufen und Verlängerungen von Kurzzeit-Visa in den Mitgliedstaaten des Schengen Raums. Die rechtliche Grundlage für das VIS bildet die Verordnung (EG) Nr. 767/2008⁴¹ (VIS-Verordnung). Das VIS besteht aus einem zentralen Visa-Informationssystem (CS-VIS), einem nationalen System (N-VIS) in jedem Mitgliedstaat und aus einer Kommunikationsinfrastruktur zwischen dem zentralen Visa-Informationssystem und den nationalen Systemen.

In Österreich ist das Bundesministerium für Inneres Verantwortlicher des VIS.

Die jeweiligen nationalen Datenschutzbehörden haben gemäß der VIS-Verordnung die Rechtmäßigkeit der Verarbeitung personenbezogener VIS -Daten auf nationaler Ebene zu überwachen, 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 erst im Dezember 2021 positiv abschließen können.

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 der Europäischen Kommission wird für das Jahr 2022 erwartet.

6.2 Europarat

Die Datenschutzbehörde vertritt die Republik Österreich im Ausschuss nach Art. 18 (T-PD) der Datenschutzkonvention des Europarates (EVS Nr. 108, BGBl. Nr. 317/1988). Im Berichtszeitraum fanden von 28. bis 30 Juni 2021 die 41. Plenarsitzung und von 17. bis 19. November 2021 die 42. Plenarsitzung des T-PD in Straßburg statt. Die Tagesordnungen sowie der zusammenfassende Bericht der Sitzung sind in englischer Sprache unter <https://www.coe.int/en/web/data-protection/consultative-committee-tpd/meetings> abrufbar.

40 <https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX%3A32013R0603>.

41 <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32008R0767>.

7 Internationale Beziehungen

Auch vergangenes Jahr fand wieder die Konferenz der Internationalen Datenschutzversammlung (Global Privacy Assembly - GPA)⁴² statt. Die GPA ist seit mehr als vier Jahrzehnten ein wichtiges globales Forum für Aufsichtsbehörden im Datenschutzbereich.

Nach einer offenen Tagung am 18. und 19. Oktober 2021, trafen sich rund 90 Mitglieder (Datenschutzbehörden) und Beobachter zu einer geschlossenen Sitzung am 20. und 21. Oktober 2021, die vom Nationalen Institut für Transparenz, Zugang zu Informationen und Schutz personenbezogener Daten (INAI) in Mexiko virtuell ausgerichtet wurde.

Im Rahmen dieser geschlossenen Sitzung wurden folgende Resolutionen⁴³ verabschiedet:

- Datenaustausch für das Gemeinwohl,
- Die digitalen Rechte von Kindern,
- Staatlicher Zugriff auf Daten, Datenschutz und Rechtsstaatlichkeit: Grundsätze für den staatlichen Zugriff auf personenbezogene Daten im Besitz des privaten Sektors zu Zwecken der nationalen und öffentlichen Sicherheit, und
- Die Zukunft der Konferenz und des Sekretariats

Die Datenschutzbehörde hat als Co-Sponsor die Resolution betreffend Staatlicher Zugriff auf Daten, Datenschutz und Rechtsstaatlichkeit unterstützt.

Die Versammlung nahm auch einen strategischen Plan für die nächsten zwei Jahre an, der sich auf die weitere Förderung des globalen Datenschutzes, die Maximierung des Einflusses der Versammlung und den Aufbau von Kapazitäten für die Mitglieder konzentriert.

In der geschlossenen Sitzung wurden zudem folgende neue Mitglieder und Beobachter begrüßt:

Neue Mitglieder: Beauftragter für Datenschutz, Abu Dhabi Global Market und das Büro des Informationsbeauftragten von Queensland, Australien.

Neue Beobachter: Nationale Datenschutzbehörde (ANPD), Brasilien; Saudi Data and Artificial Intelligence Authority, Saudi-Arabien; Ministerium für Verkehr und Kommunikation, Katar; Datenschutzbehörde, Finanzzentrum von Katar, Privacy and Civil Liberties Oversight Board, Vereinigte Staaten; Consumer Financial Protection Bureau, Vereinigte Staaten; Asiatisch-pazifisches Forum der Datenschutzbehörden (APPA) und das Inter-Amerikanische Institut für Menschenrechte (IIHR).

Neben einigen anderen personellen Neuerungen im Exekutivausschuss der Versammlung wurde die Präsidentin der mexikanischen INAI, Blance Lilia Ibarra Cadena, zur Vorsitzenden der GPA gewählt. Sie löst Elizabeth Denham, die bis November 2021 britische Informationsbeauftragte beim Information Commissioner's Office (ICO) war und ihre dreijährige Amtszeit als Vorsitzende der GPA beendete, ab.

42 <https://globalprivacyassembly.org/>.

43 <https://globalprivacyassembly.org/document-archive/adopted-resolutions/>.