

Datenschutzbericht

2022

Wien, im März 2023

Impressum

Medieninhaber, Herausgeber und Redaktion:
Datenschutzbehörde, Dr. Andrea Jelinek
(gemäß § 18ff DSG), Barichgasse 40-42, 1030 Wien
Kontakt: dsb@dsb.gv.at
Website: www.dsb.gv.at
Fotonachweis: Stefanie Korherr (Seite 6)
Gestaltung: Datenschutzbehörde
Druck: BMJ
Wien, 2023

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 Individualbeschwerden Inland.....	13
3.2.2 Rechtsauskünfte an Bürgerinnen und Bürger und FAQ zum Thema Datenschutz und Cookies.....	26
3.2.3 Genehmigungen im Internationalen Datenverkehr.....	28
3.2.4 Genehmigungen nach §§ 7 u. 8 DSG.....	29
3.2.5 Amtswegige Prüfverfahren.....	30
3.2.6 Beschwerdeverfahren vor dem Bundesverwaltungsgericht einschließlich Säumnisbeschwerden.....	32
3.2.6a Beschwerdeverfahren vor dem Bundesverwaltungsgericht in Verwaltungsstrafachen der Datenschutzbehörde.....	35
3.2.7 Verfahren über die Meldung der Verletzung des Schutzes personenbezogener Daten.....	40
3.2.8 Konsultationsverfahren.....	41
3.2.9 Anträge auf Genehmigung von Verhaltensregeln.....	44
3.2.10 Verhängung von Geldbußen durch die Österreichische Datenschutzbehörde: Erfahrungs- und Vollzugsbericht 2022.....	45
3.2.11 Stellungnahmen zu Gesetzes- und Verordnungsentwürfen.....	48

4 Wesentliche höchstgerichtliche Entscheidungen.....	49
4.1 Verfahren vor dem Verfassungsgerichtshof.....	49
4.2 Oberster Gerichtshof.....	51
4.3 Verwaltungsgerichtshof.....	55
4.4 Europäischer Gerichtshof für Menschenrechte.....	60
4.5 Europäischer Gerichtshof.....	60
5 Datenschutz-Grundverordnung und Datenschutzgesetz – Erfahrungen, legistische Maßnahmen, Projekte der Datenschutzbehörde.....	67
5.1 Allgemeine Erfahrungen der DSB im Berichtszeitraum, einschließlich Parlamentarischer Anfragen.....	67
5.1.1 So genannte „Impf-Beschwerden“.....	67
5.1.2. Strategische Befassung der Datenschutzbehörde.....	67
5.1.3. Auswirkungen der Rechtsprechung des VwGH.....	68
5.1.4. Vorabentscheidungsersuchen an den EuGH.....	69
5.1.5. Beschwerden an die Volksanwaltschaft.....	70
5.1.6. Parlamentarische Anfragen.....	70
5.2 EU-Projekt privacy4kids.....	70
6 Europäische Zusammenarbeit.....	72
6.1 Europäische Union.....	72
6.1.1 Der Europäische Datenschutzausschuss.....	72
6.1.2 Europol.....	81
6.1.3 Schengen (einschließlich Schengen Evaluierungen) sowie Visa.....	82
6.1.4 Zoll.....	83
6.1.5 Eurodac.....	84
6.2 Europarat.....	84
7 Internationale Beziehungen.....	85

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 auch im Jahr 2022 beeinflusst von der Pandemie, damit einhergehenden Fragestellungen, die unmittelbar zu beantworten waren, sowie dem Bemühen aller Mitarbeiterinnen und Mitarbeiter die Funktionsfähigkeit der Behörde zu gewährleisten.

Auch im Jahr 2022 wurden die FAQs datenschutzrechtlicher Natur die Pandemie betreffend permanent überarbeitet und ergänzt und finden sich nach wie vor 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. Nur dank ihrer kreativen Ideen, technischen Kenntnisse, ihres Fleißes und Engagements war es möglich, den Herausforderungen, mit denen die Behörde konfrontiert war, entsprechend zu begegnen und gerecht zu werden. Es wurden mehr als 6000 nationale Verfahren geführt und abgeschlossen, im internationalen Bereich haben die Kolleg:innen hervorragend und kenntnisreich mitgearbeitet.

Darüber hinaus haben die Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörde im Jahr 2022 sowohl national als auch international unzählige –viele davon im virtuellen Raum - Vorträge gehalten und (virtuelle) Veranstaltungen und Konferenzen im Bereich des Datenschutzes besucht.

Das gemeinsam mit der Universität Wien durchgeführte und von der Europäischen Kommission geförderte Projekt „privacy4kids“ wurde im Jahr 2022 erfolgreich abgeschlossen, die Ergebnisse wurden offiziell präsentiert.

Der Datenschutzbericht 2022 ist der neunte, 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 Abhelfemaßnahmen 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 Abhelfemaßnahme.

Alle Bescheide der Datenschutzbehörde 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. Seit Jahresbeginn 2023 ist es auch möglich, sich zur Beschwerdeerhebung eines Online-Formulars zu bedienen.

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 judizierte Bereich betrifft. Die Veröffentlichung erfolgt grundsätzlich dann, wenn keine Anfechtung vor dem Bundesverwaltungsgericht erfolgt.

2.2 Der Personalstand

Ende des Jahres 2022 arbeiteten 60 Mitarbeiter:innen in der Datenschutzbehörde. Dies entspricht 49,2 Vollbeschäftigungäquivalenten (VBÄ) und 10 Praktikant:innen im juristischen und im gehobenen Dienst (je 5). Diese Mitarbeiter:innen bearbeiteten unter anderem 4.890 Beschwerden im Zusammenhang mit Covid 19 und jene Beschwerden, die im „Regelbetrieb“ in der Behörde einlangten.

Neuerlich gilt der Dank Frau Bundesministerin Dr. Alma Zadić und ihrem Team, die mit der personellen, finanziellen und organisatorischen Ausstattung der Behörde dafür Sorge tragen, dass die Datenschutzbehörde ihren Aufgaben – wie in der Datenschutz-Grundverordnung vorgesehen – nachkommen kann.

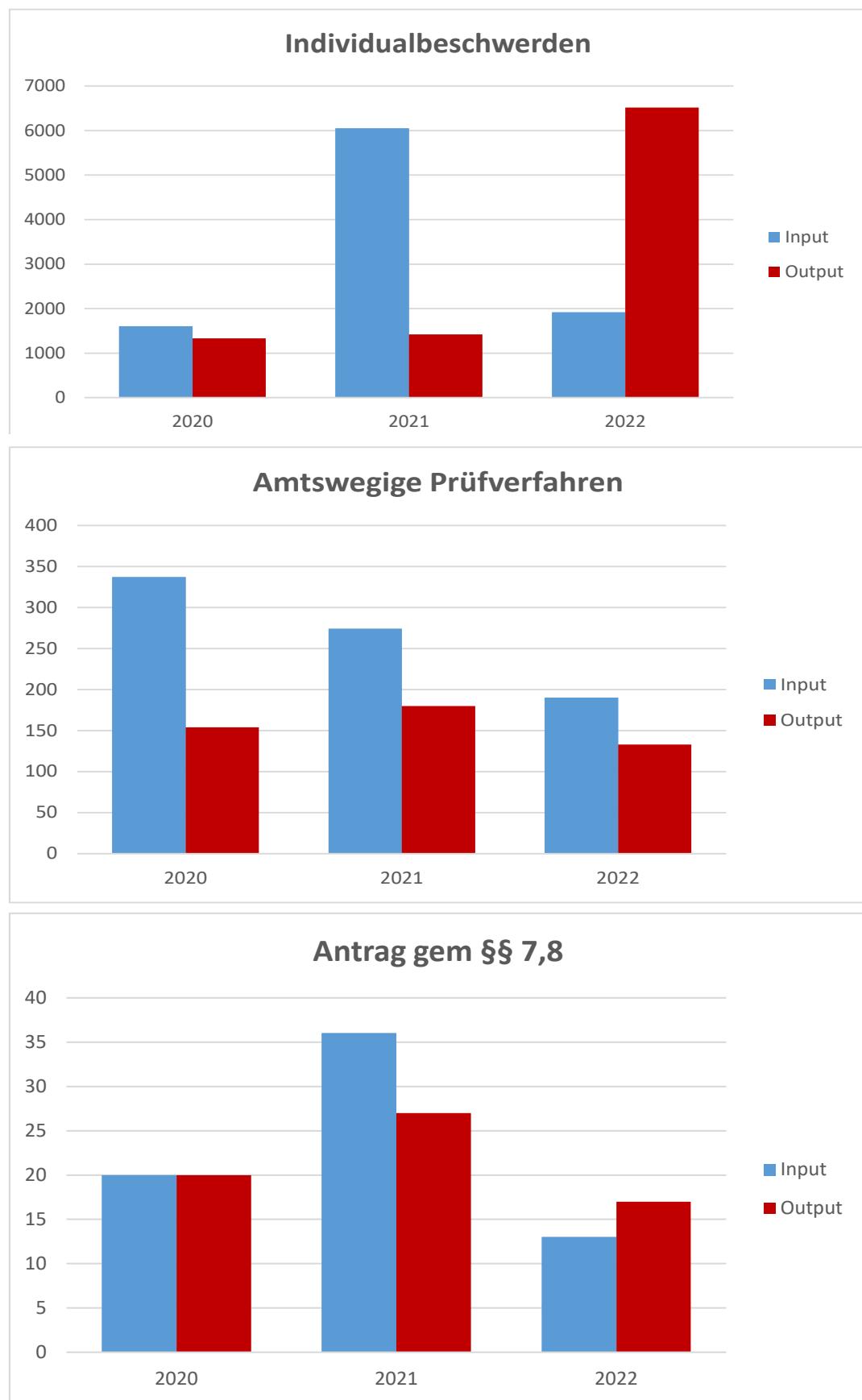
3 Tätigkeit der Datenschutzbehörde

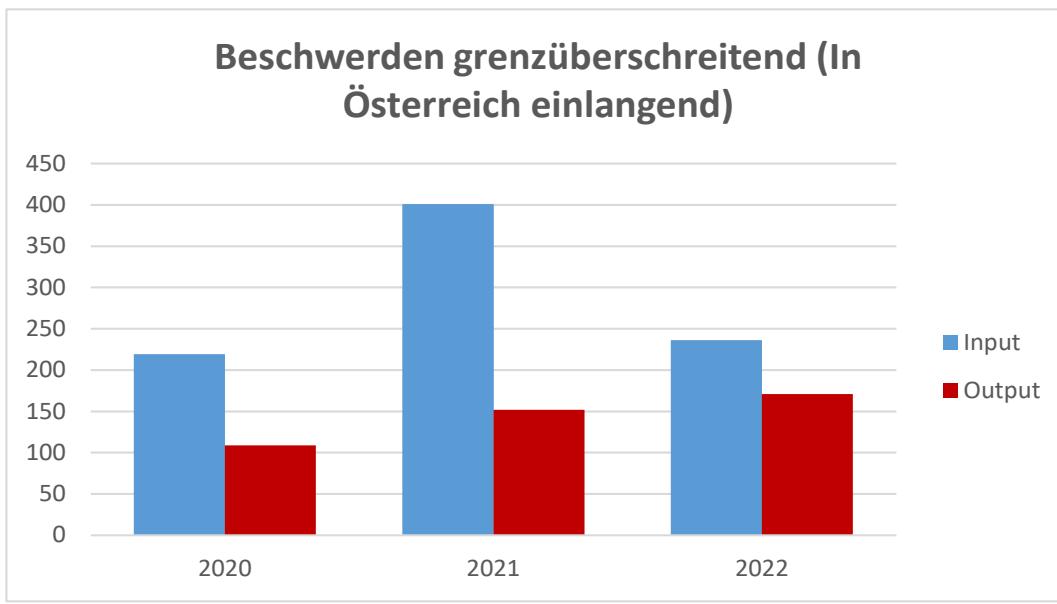
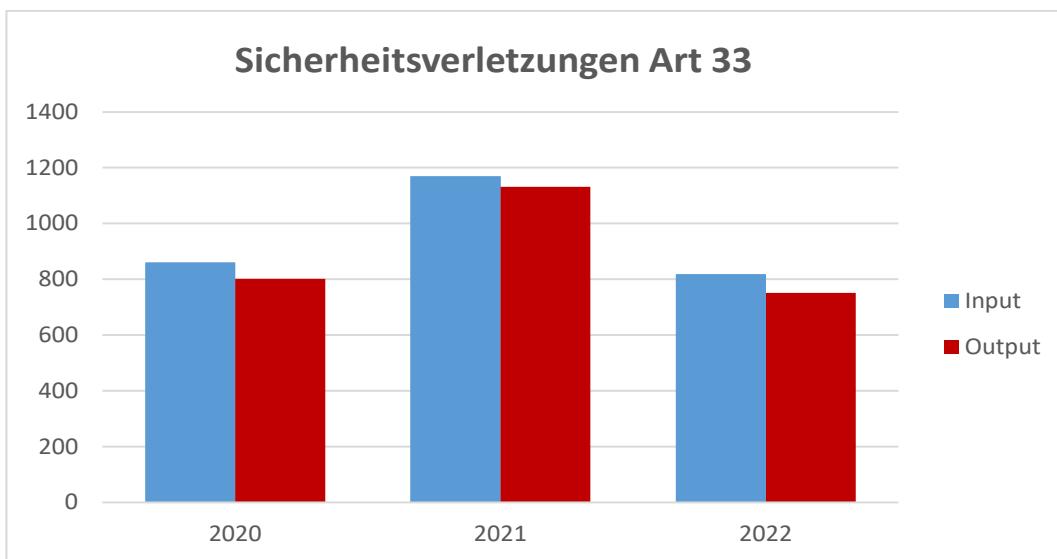
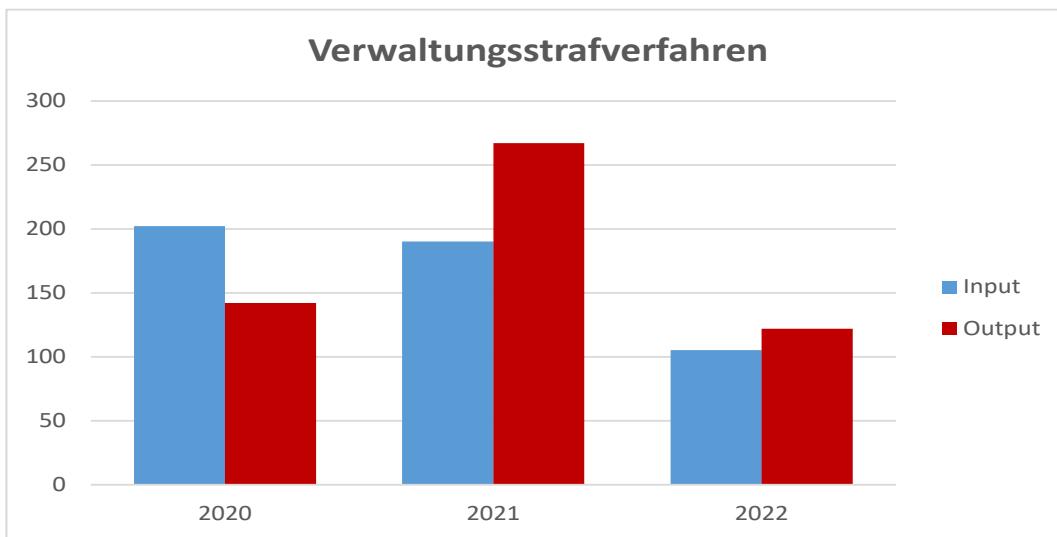
3.1 Statistische Darstellung

Tabelle 1 Anzahl der Eingangsstücke und Erledigungen

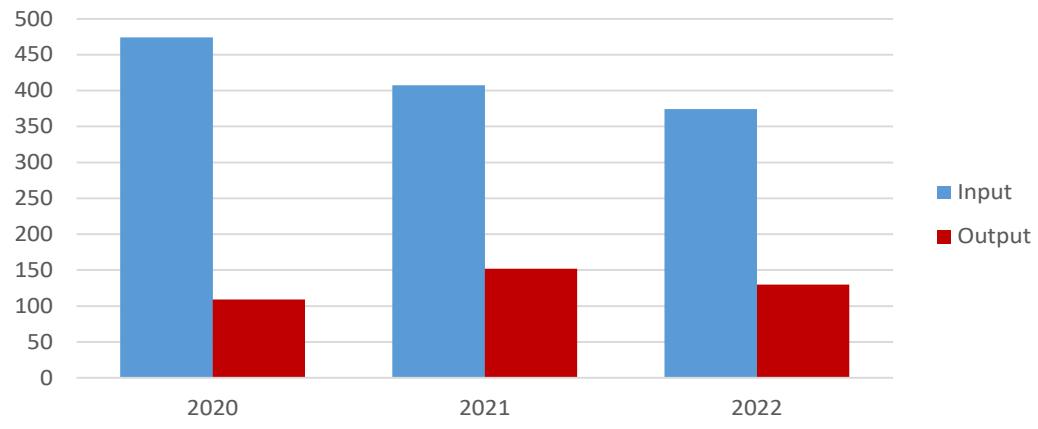
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2020	2021	2022	2020	2021	2022
Individualbeschwerden	1603	6051	1915	1332	1421	6517
Erledigungsart der Individualbeschwerden				852 Bescheide 480 Einstellungen	1036 Bescheide 385 Einstellungen	4806 Bescheide 1712 Einstellungen
Beschwerden Grenzüberschreitend (im Ausland einlangend)	474	407	374	403	226	130
Beschwerden Grenzüberschreitend (in Österreich einlangend)	219	401	236	109	152	171
Amtswegige Prüfverfahren	337	274	190	154	180	133
Erledigungsart der Amtswegigen Prüfverfahren					10 Bescheide 170 Einstellungen	11 Bescheide 122 Einstellungen
Genehmigungen nach §§ 7 und 8 DSG (wissenschaftliche Forschung u. Statistik)	20	36	13	20	27	17
Genehmigungen im Internationalen Datenverkehr	0	0	1	0	0	1
Auskunft Schengen	127	117	746	127	117	746
Verwaltungsstrafverfahren	202	190	105	142	267	122
Erledigungsart der Verwaltungsstrafverfahren					56 Bescheide 211 Einstellungen	63 Bescheide 59 Einstellungen

Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2020	2021	2022	2020	2021	2022
Verfahren vor dem Bundesverwaltungsgericht	319	511	1193			
- Davon Bescheidbeschwerden			1156			
- Davon Säumnisbeschwerden			37			
Sicherheitsverletzungen § 95a	60	55	25	61	50	25
Sicherheitsverletzungen Art 33	860	1169	818	802	1131	751
Sicherheitsverletzungen grenzüberschreitend (in Österreich eingelangend)	14	30	15	10	18	9
Sicherheitsverletzungen grenzüberschreitend (im Ausland eingelangend)	76	62	20	45	45	3
Rechtsauskünfte	3166	3257	3069	3227	3257	3069
Allgemeine Anfragen Ausland	59	32	52	47	34	52
Amtshilfeersuchen Ausland		228	56		137	56
Anträge auf Genehmigung von Verhaltensregeln	2	4	2	2	3	5
Genehmigung BCR (International)	5	0	0	2	0	2
Konsultationsverfahren	1	1	3	1	1	3
Datenschutzbeauftragte	632	626	602	632	626	602
Verkehr mit Behörden	140	137	239	140	137	239

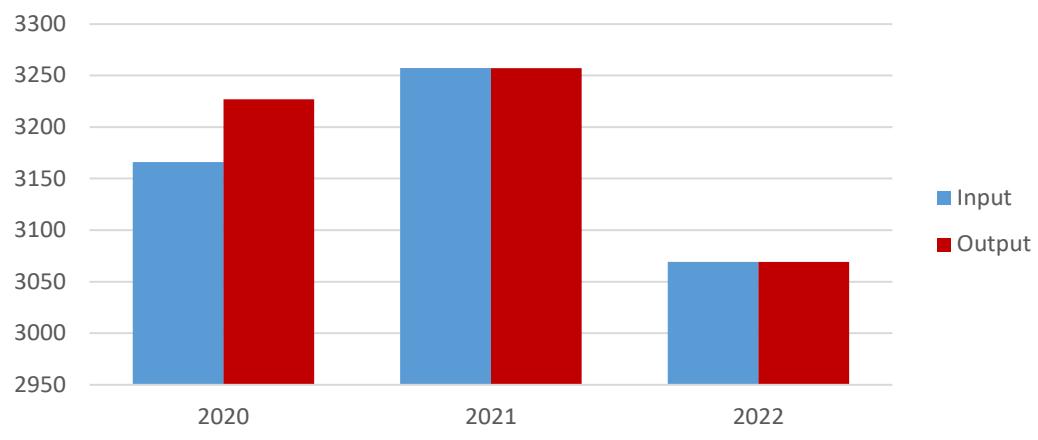




Beschwerden grenzüberschreitend (Im Ausland einlangend)



Rechtsauskünfte



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 Prüforganen wie Rechnungshof und Volksanwaltschaft)¹
- die Gerichtsbarkeit, soweit sie justizielle Aufgaben (einschließlich Angelegenheiten der Justizverwaltung, die durch Richterkollegien entschieden werden, Art. 87 Abs. 2 B-VG) wahrt, 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: Zur Tragweite justizieller Tätigkeiten siehe das Urteil des EuGH zu C-245/20.

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

4 Hinweis: §9 Abs. 1 DSG wurde mit Erkenntnis des VfGH vom 14.12.2022 als verfassungswidrig aufgehoben. Die Aufhebung tritt mit Ablauf des 30.06.2024 in Kraft.

Im Verfahren wegen Verletzung der Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und - fallweise - 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 Staatschutzes, 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 einzutreten („kommissarischer Rechtsschutz“, vgl. insbesondere § 42 Abs. 8 und 9 DSG).

Praxis der Beschwerdeverfahren im Jahr 2022

Im Berichtsjahr 2022 wurden insgesamt 1.915 Individualbeschwerden bei der Datenschutzbehörde eingebracht. 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 2022

Die DSB hat in ihrer öffentlich zugänglichen Entscheidungsdokumentation (im Rahmen des Rechtsinformationssystems des Bundes – RIS;) aus dem Jahr 2022 acht 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 2022 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 27. Jänner 2022, GZ: 2021-0.785.022 (Beschwerdegegnerin ist nicht Verantwortliche, wenn Mitarbeiter aus eigenem Interesse ELGA-Abfragen tätigen)

Der Beschwerdeführer behauptete, dass es durch zwei Mitarbeiterinnen der Beschwerdegegnerin zu nicht autorisierten Zugriffen auf seine Medikations- und Impfstatusdaten gekommen sei. Die Beschwerdegegnerin argumentierte, dass die Zugriffe ohne ihr Wissen erfolgt seien, aber keine Ausdrucke angefertigt oder Daten an Dritte weitergeleitet worden wären. Auch müssten alle Mitarbeiter zu Beginn des Dienstverhältnisses eine Geheimhaltungsvereinbarung samt Datenschutzerklärung unterfertigen.

Im gegenständlichen Fall ging aus dem Beschwerdevorbringen eindeutig hervor, dass der Beschwerdeführer gegen die Beschwerdegegnerin selbst vorgehen wollte. Da die Mitarbeiterinnen, die die Abfragen in der ELGA-Akte des Beschwerdeführers durchgeführt haben, nach Ansicht der Datenschutzbehörde als Verantwortliche gemäß Art. 4 Z 7 DSGVO zu qualifizieren waren, wäre die Beschwerde gegen die Mitarbeiterinnen selbst zu richten gewesen (vgl. dazu auch das Erkenntnis des BVwG vom 29. Jänner 2021, GZ: W2112232168).

Unter Berücksichtigung der ständigen Rechtsprechung des VwGH (vgl. 07.03.2016, Ra 2016/02/0030) hielt die Datenschutzbehörde weiters fest, dass ein wirksames Kontrollsyste nicht die ständige Beaufsichtigung des Arbeitnehmers verlangt, sodass keinerlei Anhaltspunkte vorlagen, dass die gegenständlichen Datenzugriffe durch mangelnde Kontrollmaßnahmen der Beschwerdegegnerin ermöglicht worden sind. Die Beschwerde war daher abzuweisen.

Der Bescheid ist nicht rechtskräftig.

2. Bescheid vom 7. Februar 2022, GZ: 2022-0.094.281 (Auskunftsmaßnahmen gemäß Art. 15 DSGVO durch einen Kassenplanstellennachfolger gemäß § 51 Abs. 4 ÄrzteG)

Der Beschwerdegegner, ein zugelassener Facharzt für Lungenerkrankungen, hatte von seinem pensionierten Vorgänger die Patientendokumentation übernommen, in welcher sich auch personenbezogene Daten des Beschwerdeführers befanden.

Der Beschwerdeführer, der beim Vorgänger in Behandlung gewesen war, begehrte vom Beschwerdegegner Auskunft über seine personenbezogenen Daten. Die Patientendaten des Beschwerdeführers waren vom Vorgänger des Beschwerdegegners allerdings Großteils hand-

schriftlich auf Karteikarten erfasst worden. Nach der Übermittlung der Karteikarten durch den Beschwerdegegner monierte der Beschwerdeführer die Unvollständigkeit der erteilten Auskunft. So habe es der Beschwerdegegner unterlassen, die unleserlichen Passagen auf den Karteikarten und die Abkürzungen zu erläutern und seien ihm keine Daten zu einem Inhalationsgerät, das er vom Vorgänger des Beschwerdegegners erhalten habe, beauskunftet worden.

Die Datenschutzbehörde stellte fest, dass das an den Beschwerdegegner gerichtete Begehren, handschriftliche Patientendaten zu „interpretieren“, nicht vom Recht auf Auskunft gedeckt ist. Insbesondere könnten dem Beschwerdegegner bei einer nachträglichen „Interpretation“ der unleserlichen Passagen der Karteikarten gesundheitsgefährdende Fehler unterlaufen, weshalb die vom Beschwerdeführer verlangte korrekte Interpretation der handschriftlichen Notizen nicht geboten ist. Nach Ansicht der Datenschutzbehörde kam der Beschwerdegegner durch die Übermittlung der Karteikarten seinen Verpflichtungen im Sinne des Art. 12 Abs. 1 DSGVO und Art. 15 DSGVO nach. Hinsichtlich der behaupteten Unvollständigkeit der Auskunft im Zusammenhang mit dem Inhalationsgerät wies die Datenschutzbehörde unter Verweis auf die glaubwürdige Darlegung des Beschwerdegegners und das Erkenntnis des BVwG vom 27. September 2019, GZ: W101 2139434-1, wonach aus dem Recht auf Auskunft keine nachträgliche Erhebungspflicht des Verantwortlichen abgeleitet werden kann, die Beschwerde ab.

Der Bescheid ist nicht rechtskräftig.

3. Bescheid vom 14. Februar, GZ: 2022-0.083.310 (Abweisung des Antrages auf Erlassung eines Mandatsbescheides nach § 22 DSG)

Die Datenschutzbehörde ist gemäß § 22 DSG grundsätzlich berechtigt, eine Datenverarbeitung mit Mandatsbescheid zu untersagen, sofern eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen des Betroffenen (Gefahr im Verzug) vorliegt.

Im gegenständlichen Verfahren setzte sich die Datenschutzbehörde mit einem Antrag auf Erlassung eines Mandatsbescheides wegen behaupteter Gefahr im Verzug im Zusammenhang mit einer von einem Untersuchungsausschuss beantragten Aktenübermittlung durch einen Bundesminister gemäß § 25 VO-UA auseinander.

Zunächst gelangte die Datenschutzbehörde zur Ansicht, dass es grundsätzlich möglich ist, Beschwerden im Zusammenhang mit einer Aktenvorlage durch ein informationspflichtiges Verwaltungsorgan an einen Untersuchungsausschuss bei der Datenschutzbehörde einzubringen. Die Datenschutzbehörde wies jedoch darauf hin, dass ihre Rolle in einem solchen Fall auf eine ex post-Kontrolle beschränkt ist.

Der Antragsteller begründete seinen Antrag auf Erlassung eines Mandatsbescheides damit, dass ihn betreffende Informationen bzw. Unterlagen durch Dritte (Mitglieder des Untersuchungsausschusses) veröffentlicht werden könnten. Der Antragsteller vermochte allerdings nicht darzulegen, inwieweit die beanstandete Datenverarbeitung durch den Antragsgegner, hier der Untersuchungsausschuss, seine Geheimhaltungsinteressen verletzen würde.

Die Datenschutzbehörde hielt fest, dass es sich bei der Befürchtung, Mitglieder des Untersuchungsausschusses würden im Rahmen der Tätigkeit für den Untersuchungsausschuss bekannt gewordene Informationen Dritten gegenüber offenlegen, lediglich um eine hypothetische Erwähnung handelt, weshalb der Antrag auf Erlassung eines Mandatsbescheides abgewiesen wurde.

Der Bescheid ist rechtskräftig.

4. Bescheid vom 1. März 2022, GZ: 2021-0.789.408 (Einsatz eines GPS-Systems im Dienstfahrzeug)

Der Beschwerdeführer war bei der Beschwerdegegnerin als Kundendiensttechniker angestellt. In diesem Zusammenhang wurde ihm ein Fahrzeug, in welches ein GPS-Gerät eingebaut war und das er auch für private Fahrten nutzen durfte, zur Verfügung gestellt. Das GPS-Gerät wurde durch Start der Zündung des Fahrzeugs aktiviert und durch Ausschalten der Zündung deaktiviert. Zusätzlich befand sich im Fahrzeug ein Schalter, mit welchem das GPS-Gerät für private Fahrten deaktiviert werden konnte.

Die Datenschutzbehörde kam im Rahmen der Interessenabwägung zum Ergebnis, dass es an der Erforderlichkeit bzw. Verhältnismäßigkeit der Datenverarbeitung durch das GPS-Gerät mangelte. Zwar wurde seitens der Datenschutzbehörde nicht verkannt, dass das GPS-Gerät eine administrative Erleichterung und eine ökonomische Entlastung für die Beschwerdegegnerin darstellt, dies alleine vermochte jedoch eine Berufung auf Art. 6 Abs. 1 lit. f DSGVO nicht zu rechtfertigen, da der Zweck auch durch gelindere Mittel, welche eine geringere Datenverarbeitung mit sich bringen, erreicht hätte werden können. Ebenso wenig konnte die Datenverarbeitung nach Ansicht der Datenschutzbehörde auf Art. 6 Abs. 1 lit. c DSGVO bzw. auf die von der Beschwerdegegnerin vorgebrachten Bestimmungen des Arbeitszeitgesetzes gestützt werden. Der Beschwerde wurde daher stattgegeben.

Der Bescheid ist nicht rechtskräftig.

5. Bescheid vom 1. Juni 2022, GZ: 2022-0.345.404 (Rechtmäßigkeit einer Datenverarbeitung durch den Einsatz von Cookies)

Die Beschwerdegegnerin ist Betreiberin einer Webseite für Sportartikel. Als die Beschwerdeführerin diese Webseite besuchte, interagierte sie nicht mit dem Cookie-Banner bzw. erteilte keine Einwilligung. Nach Aufruf der Webseite wurde der Beschwerdeführerin dennoch Werbung der Beschwerdegegnerin auf anderen Webseiten angezeigt.

Beim Besuch der Webseite der Beschwerdegegnerin wurden Cookies, u.a. für die Dienste Criteo, Google Analytics und Google Ads, im Browser bzw. am Endgerät der Beschwerdeführerin gesetzt. Als Konsequenz wurden zahlreiche Informationen vom Browser an die Server von Werbepartnern verschickt, unter anderem die einzelnen Produktseiten, die die Beschwerdeführerin besucht hatte, sowie einzigartige Nutzer-Identifikations-Nummern, die am Endgerät der Beschwerdeführerin gespeichert waren.

Die Datenschutzbehörde hielt zunächst fest, dass die gegenständlichen Nutzer-Identifikations-Nummern als personenbezogene Daten gemäß Art. 4 Z 1 DSGVO zu qualifizieren sind. Durch Kombination weiterer Elemente entstand ein digitaler Fußabdruck und so war es umso wahrscheinlicher, dass die Beschwerdeführerin letztlich (an irgendeiner Stelle der Verarbeitungskette) identifiziert werden konnte. Diese Beurteilung entspricht auch der Rechtsauffassung des Europäischen Datenschutzbeauftragten. Zudem konnte von der Beschwerdegegnerin im Rahmen ihrer Rechenschaftspflicht kein Beweis erbracht werden, dass die Werbepartner die Informationen nicht mit der Beschwerdeführerin in Verbindung bringen können.

Dies hatte zur Folge, dass der Beschwerdeführerin personalisierte Werbung angezeigt wurde. Das Setzen oder Auslesen von Cookies, welche dem Ausspielen von personalisierter Werbung dienen oder die zu diesen Zwecken das Sammeln des Surfverhaltens ermöglichen, ist aus technischer Sicht nicht notwendig, weshalb jedenfalls eine vorherige Einwilligung der Beschwerdeführerin erforderlich gewesen wäre.

Demzufolge konnte die dem Setzen oder Auslesen von Cookies folgende Datenverarbeitung – also das Profiling – mangels Einwilligung nicht auf Art. 6 Abs. 1 lit. a DSGVO gestützt werden. Ebenso wenig kam Art. 6 Abs. 1 lit. f DSGVO in Betracht, da eine Interessenabwägung nicht gegen die betroffene Person ausschlagen kann, wenn im Vorfeld gegen sekundärrechtliche Normen bzw. das TKG 2021 verstoßen wurde.

Der Bescheid ist nicht rechtskräftig.

6. Bescheid vom 21. Juni 2022, GZ: 2022-0.191.287 (Manuelles Einlegen von Werbematerial in voraddressiertes Briefkuvert)

Die beschwerdeführende Partei sah sich u.a. in ihrem Recht auf Geheimhaltung verletzt, da sie bei der Beschwerdegegnerin – einem Unternehmen zur Erbringung von Postdienstleistungen – einen Nachsendeauftrag eingerichtet und in weiterer Folge ein postalisches Bestätigungsschreiben erhalten hatte, dem nichtpersonalisierte Werbematerialien beigelegt waren, obwohl sie die Verwendung ihrer personenbezogenen Daten für Marketingzwecke Dritter auf dem Nachsendeauftragsformular untersagt hatte. Die Beschwerdegegnerin legte im Ermittlungsverfahren dar, dass die Werbematerialien manuell in den bereits voraddressierten Briefumschlag gelegt worden waren.

Die Datenschutzbehörde hielt zunächst fest, dass der Geheimhaltungsanspruch nach § 1 Abs. 1 DSG – anders als Betroffenenrechte nach der DSGVO – unabhängig von der Art der Datenverarbeitung besteht. Jedoch setzt auch der Anwendungsbereich von § 1 DSG immer eine Verarbeitung personenbezogener Daten der betroffenen Person voraus. Beim verfahrensgegenständlichen Vorgang, der manuellen Beilegung von Werbematerialien in einen Briefumschlag, wurden jedoch keine personenbezogenen Daten des Beschwerdeführers verarbeitet, weshalb auch kein datenschutzrechtlich relevanter Verarbeitungsvorgang vorliegt. Da sich auch keine Anhaltspunkte ergeben haben, dass personenbezogene Daten der beschwerdeführenden Partei an Dritte für deren Marketingzwecke weitergegeben worden waren, wurde die Beschwerde abgewiesen.

Der Bescheid ist nicht rechtskräftig.

7. Beschwerdevorentscheidung vom 29. Juli 2022, GZ: 2022-0.502.311 (Aufnahme von Ergebnisprotokollen des ersten Teiles von Mitarbeitergesprächen nach BDG in den Personalakt)

Der Beschwerdeführer, ein in einem öffentlich-rechtlichen Dienstverhältnis zum Bund stehender Beamter, hatte im Rahmen einer Einschau in seinen Personalakt festgestellt, dass seitens seiner Dienststelle die Ergebnisprotokolle der ersten Teile mehrerer Mitarbeitergespräche der letzten Jahre in seinen Personalakt aufgenommen worden waren.

Nach § 45a Abs. 1 des Beamten-Dienstrechtsgegesetzes hat der unmittelbar mit der Fachaufsicht betraute Vorgesetzte einmal jährlich mit jedem seiner Mitarbeiter ein Mitarbeitergespräch zu führen. Dieses setzt sich gemäß Abs. 2 leg. cit. aus zwei Teilen zusammen. Wenngleich die Ergebnisse beider Teile schriftlich zusammenzufassen sind, und das Ergebnisprotokoll des zweiten Teiles in den Personalakt aufzunehmen ist, hat je eine Ausfertigung des Ergebnisses des ersten Teiles beim Mitarbeiter und seinem Vorgesetzten zu verbleiben und darf dieses nicht weitergegeben werden. Die Aufnahme der Ergebnisprotokolle des ersten Teiles der Gespräche in den Personalakt des Beschwerdeführers stellte sohin eine Verletzung im Recht auf Geheimhaltung dar.

Der Bescheid ist rechtskräftig.

8. Bescheid vom 7. September 2022, GZ: 2022-0.560.569 (Keine Beschwerde gegen sich selbst)

Im gegenständlichen Verfahren erhab der Beschwerdeführer eine Beschwerde gegen sich selbst und ersuchte die Datenschutzbehörde um Klärung, ob eine Datenschutzverletzung durch die Verwendung des Beschwerdeformulars der Datenschutzbehörde, konkret durch die Angabe der E-Mail-Adresse und Telefonnummer eines Beschwerdegegners, möglich sei.

Die Datenschutzbehörde setzte sich mit dem Beschwerderecht einer betroffenen Person gemäß Art. 77 Abs. 1 DSGVO und § 24 Abs. 1 DSG auseinander und hielt fest, dass eine notwendige Voraussetzung für die Geltendmachung des Beschwerderechts die Betroffenheit der beschwerdeführenden Person durch die Verarbeitung ist. Es handelt sich daher um ein Recht, das einer betroffenen Person zusteht, nicht jedoch beispielsweise einem Verantwortlichen oder Auftragsverarbeiter. Gegenständlich ergab sich aus dem Vorbringen des Beschwerdeführers, dass dieser nicht selbst die betroffene Person war, sondern vielmehr die personenbezogenen Daten des Beschwerdegegners – als die eigentlich betroffene Person – womöglich widerrechtlich offengelegt hatte und nun gegen sich selbst eine Beschwerde einbrachte.

Mangels persönlicher Betroffenheit des Beschwerdeführers war dieser nicht zur Einbringung der gegenständlichen Beschwerde legitimiert, weshalb die Datenschutzbehörde die Beschwerde zurückwies.

Der Bescheid ist rechtskräftig.

9. Bescheid vom 13. September 2022, GZ: 2021-0.848.839 (Weitergabe der Telefonnummer eines Schülers durch die Volksschule)

Die Datenschutzbehörde hatte in diesem Verfahren zu beurteilen, ob die Weitergabe der Telefonnummer der Erziehungsberechtigten eines Schülers durch die Direktorin der Volksschule anlässlich einer Rauferei an die Erziehungsberechtigten des beteiligten Mitschülers rechtmäßig erfolgte.

Die Direktorin hatte die zuständige Klassenlehrerin zur Weitergabe der Telefonnummer angewiesen und sich im Verfahren auf die Wahrung der berechtigten Interessen des Mitschülers, nämlich eine allfällige Entschädigung für seine beschädigte Brille zu erhalten, berufen.

Die Datenschutzbehörde gab der Beschwerde statt und kam zum Ergebnis, dass die Weitergabe der Telefonnummer die Beschwerdeführerin in ihrem Recht auf Geheimhaltung verletzt hat. Die Direktorin war als datenschutzrechtliche Verantwortliche nach Art. 4 Z 7 DSGVO anzusehen und erfolgte die Weitergabe der Telefonnummer als hoheitliche Datenverarbeitung. Da staatliche Eingriffe gemäß § 1 Abs. 2 DSG nur auf Grund von Gesetzen zulässig sind und aus dem anzuwendenden Schulunterrichtsgesetz keine entsprechende Verarbeitungsermächtigung abgeleitet werden konnte, erfolgte die Weitergabe der Telefonnummer unrechtmäßig.

Der Bescheid ist nicht rechtskräftig.

10. Bescheid vom 19. Oktober 2022, GZ: 2022-0.360.359 (Verarbeitung biometrischer Daten mittels Handvenenscanner; Videoüberwachung am Arbeitsplatz)

Der Beschwerdeführer, ein ehemaliger Mitarbeiter der Beschwerdegegnerin, erachtete sich im Recht auf Geheimhaltung verletzt, weil die Beschwerdegegnerin seine biometrischen Daten mittels eines Handvenenscanners verarbeitet und ihn mit Videoüberwachungskameras erfasst hatte.

Die Beschwerdegegnerin betreibt ein Gastronomielokal in Wien. Sie verwendet dort einen Handvenenscanner, welcher mittels Infrarotlicht das Handvenenmuster der vor den Scanner gehaltenen Hand misst. Der Handvenenscanner wird verwendet, damit die Mitarbeiter der Beschwerdegegnerin eindeutig identifiziert werden und Einsicht in ihre arbeitsvertraglichen Dokumente nehmen und ihre monatlichen Arbeitszeitaufzeichnungen kontrollieren und abzeichnen können.

Des Weiteren betreibt die Beschwerdegegnerin 29 Videoüberwachungskameras an diesem Standort. Zwei davon nehmen auch Bereiche der Küche auf, in welcher der Beschwerdeführer als Koch hauptsächlich tätig war.

Die Datenschutzbehörde gab der Beschwerde teilweise statt und stellte fest, dass die Beschwerdegegnerin den Beschwerdeführer dadurch im Recht auf Geheimhaltung verletzt hat, indem sie seine biometrischen personenbezogenen Daten unrechtmäßig verarbeitet und ihn mit zwei Kameras in der Küche erfasst hat.

Die Beschwerdegegnerin stützte sich bei Verarbeitung der biometrischen Daten, die als Daten besonderer Kategorie gemäß Art. 9 Abs. 1 DSGVO zu qualifizieren sind, auf den Ausnahmetatbestand des Art. 9 Abs. 2 lit. a DSGVO (Einwilligung).

Die Datenschutzbehörde hielt fest, dass die eingeholte Einwilligung jedoch nicht rechtskonform erteilt wurde. So wurde schon im Arbeitsvertrag festgehalten, dass der Beschwerdeführer für die gesamte Zeit des bestehenden Arbeitsverhältnisses seine „ausdrückliche Zustimmung zur Einführung und Verwendung eines auf biometrischem Handflächenscanning beruhenden Systems für die Unterschriftenleistung für betriebliche Dokumente im Unternehmen“ erteilt hat.

Die Datenschutzbehörde kam zum Ergebnis, dass die später erfolgte Einwilligung am Terminal des Handvenenscanners vom Beschwerdeführer nicht freiwillig erteilt werden konnte und war die damit einhergehende Datenverarbeitung unrechtmäßig.

Der Beschwerde wurde auch hinsichtlich der in der Küche angebrachten Videoüberwachungskameras stattgegeben, da nach Ansicht der Datenschutzbehörde die Geheimhaltungsinteressen des Beschwerdeführers gegenüber den Interessen der Beschwerdegegnerin an der Aufklärung und Verhinderung von etwaigen Diebstählen und Einbrüchen und Beschädigungen bei der Anlieferung/Entsorgung überwiegen. Dabei hob die Datenschutzbehörde hervor, dass es sich bei Bildverarbeitungen im Beschäftigungskontext um besonders intensive Privatrechtseingriffe handelt. Es war nicht erkennbar, weshalb zum Schutz der vom Beschwerdegegner angegebenen Ziele die Küchenarbeitsbereiche, in welchen sich der Beschwerdeführer hauptsächlich zur Verrichtung seiner Arbeit aufhielt, von Videokameras erfasst werden müssen. So wäre es etwa möglich, vereinzelt Kameras in jenen Räumen, in welchen sich wertvolle Güter befinden, zu installieren und auf Flucht- und Entsorgungswege zu richten, um die von der Beschwerdegegnerin angeführten Zwecke zu verwirklichen. Der Beschwerdegegnerin wurde der Betrieb der beiden Videoüberwachungskameras untersagt und ihr darüber hinaus aufgetragen, ihre Videoüberwachungsanlage gemäß Art. 13 DSGVO geeignet zu kennzeichnen.

Der Bescheid ist nicht rechtskräftig.

11. Bescheid vom 7. Dezember 2022, GZ: 2022-0.737.249 (Unzulässigkeit der Kontrolle von E-Mail-Protokollen)

Das Verfahren wurde auf Grund der Beschwerde dreier Angestellter gegen die Beschwerdegegnerin eingeleitet, welche eine Verletzung im Grundrecht auf Geheimhaltung behaupteten. Zusammengefasst wurde vorgebracht, dass die Beschwerdegegnerin – ohne Einwilligung und Kenntnis der Beschwerdeführer – die technischen Mail-Serverprotokolle aller 6.000 Angestellten auf eine spezifische Empfängerdomain überprüft habe. Anlass für diese Kontrollmaßnahme sei der Verdacht einer Verletzung des Geschäftsgeheimnisses gewesen.

Die Datenschutzbehörde führte im vorliegenden Fall zunächst aus, dass die Beschwerdegegnerin – eine juristische Person des öffentlichen Rechts – eine gesetzliche Grundlage benötigt, um eine solche Kontrollmaßnahme durchzuführen. Eine hinreichend determinierte gesetzliche Grundlage für eine derartige Kontrollmaßnahme war im gegenständlichen Fall allerdings nicht ersichtlich. Unter der Annahme, dass die Beschwerdegegnerin sich auf berechtigte Interessen iSd § 1 Abs. 2 DSG bzw. Art. 6 Abs. 1 lit. f DSGVO stützen wollte, hielt die Datenschutzbehörde fest, dass eine solche Interessenabwägung gegen die Beschwerdegegnerin ausfallen würde, da die Kontrollmaßnahme erst sechs Monate nach dem anlassgebenden Vorfall stattgefunden hat und auf Grund des fehlenden zeitlichen Konnexes nicht verhältnismäßig gewesen wäre. Im Rahmen der Interessenabwägung wäre zudem auch zu berücksichtigen gewesen, dass keine gültige Zustimmung des Betriebsrats vorhanden war, die nach Ansicht der Datenschutzbehörde aber erforderlich ist.

Im Ergebnis wurde ausgesprochen, dass eine Verletzung im Recht auf Geheimhaltung vorliegt.

Dieser Bescheid ist nicht rechtskräftig.

12. Bescheid vom 15. Dezember 2022, GZ: 2022-0.876.190 (Datenverarbeitungen durch eine in Wien ansässige Botschaft eines Drittstaates)

Die Datenschutzbehörde hatte sich mit der Frage zu befassen, inwiefern vor der österreichischen Datenschutzbehörde eine Rechtsverletzung durch eine in Wien ansässige Botschaft eines Drittstaates geltend gemacht werden kann.

Die Datenschutzbehörde erwog bei ihrer Beurteilung ihre Zuständigkeit im Hoheitsgebiet der Republik Österreich gemäß Art. 55 Abs. 1 DSGVO und berücksichtigte hierbei, dass Botschaften nach dem modernen Völkerrecht nicht Exklaven eines anderen Staates sind, sondern territorial dem Empfangsstaat zugeordnet werden. Allerdings ergibt sich bereits aus der Ausnahme des Art. 55 Abs. 2 DSGVO die mangelnde Zuständigkeit der österreichischen Datenschutzbehörde gegenüber Datenverarbeitungen durch Behörden oder private Stellen anderer Mitgliedstaaten auf der Grundlage von Art. 6 Abs. 1 lit. c oder e DSGVO. Folglich muss dies auch für Behörden oder private Stellen gelten, deren Datenverarbeitungen einem Drittstaat zuzurechnen sind.

Zu beachten war überdies das Wiener Übereinkommen über diplomatische Beziehungen, welches sowohl von der Republik Österreich als auch dem betreffenden Drittstaat ratifiziert ist. Gemäß dessen Art. 31 Abs. 1 genießen Diplomaten u.a. Immunität von der Verwaltungsgerichtsbarkeit des Empfangsstaates, auch wenn sie gemäß Art. 41 Abs. 1 verpflichtet sind, die Gesetze und andere Rechtsvorschriften des Empfangsstaates – sohin auch die DSGVO, die als unmittelbar anwendbarer Rechtsakt der Europäischen Union innerstaatlichen Gesetzen gleichgestellt ist – zu beachten. Kraft dieser völkerrechtlichen Regelung kann der von dem Drittstaat entsendete Botschafter bzw. die ihm unterstehende Mission daher von der österreichischen Datenschutzbehörde nicht belangt werden. Im Ergebnis war die Beschwerde somit zurückzuweisen.

Der Bescheid ist rechtskräftig.

13. Bescheid vom 22. Dezember 2021, GZ: 2021-0.586.257 (Google Analytics)

In diesem Verfahren hatte sich die Datenschutzbehörde mit der Frage zu befassen, ob der Einsatz von Google Analytics mit den in Kapitel V der DSGVO normierten Vorgaben für den Internationalen Datenverkehr vereinbar ist. Die Beschwerdegegner waren der Betreiber der Webseite und Google LLC. Weitere Aspekte der DSGVO – wie etwa die Rechtmäßigkeit nach Art. 6 Abs. 1 DSGVO – waren nicht vom Beschwerdegegenstand umfasst.

Bei Google Analytics handelt es sich um ein Google-Tool, mit dem Betreiber einer Webseite detaillierte Berichte über das Nutzerverhalten von Webseiten-Besuchern erstellen können. Beim Aufruf einer Webseite, die Google Analytics verwendet, wird dem Browser des Besuchers eine Google Analytics Kennnummer zugeordnet. Besucher können anhand dieser Kennnummer individualisiert und unterschiedlich behandelt werden. Zusätzlich besteht die Möglichkeit, diese Kennnummer mit weiteren Informationen zu kombinieren, wie etwa mit der IP-Adresse oder gewissen Browserdaten. Durch diese Kombination entsteht ein einzigartiger digitaler Fußabdruck, der dem Benutzer des Browsers zugeordnet werden kann. Wenn ein Besucher während des Aufrufs einer solchen Webseite in sein Google Konto eingeloggt ist, kann die Information über den Webseitenbesuch – zumindest unter gewissen Voraussetzungen – auch dem jeweiligen Google Konto zugeordnet werden.

Die Datenschutzbehörde hielt zunächst fest, dass dieser digitale Fußabdruck ein personenbezogenes Datum darstellt. Konkret handelt es sich um ein personenbezogenes Datum jenes Benutzers, der das Endgerät bzw. den Browser am wahrscheinlichsten verwendet hat. Dies war im gegenständlichen Fall die beschwerdeführende Partei, zumal diese während des Aufrufs der Webseite in ihrem Google-Konto eingeloggt war. Nach Auffassung der Datenschutzbehörde können aber auch einzelne Elemente des digitalen Fußabdrucks – wie etwa die Online-Kennung in Form der Google-Analytics Kennnummer – ein personenbezogenes Datum darstellen. Diese Ansicht wurde auch seitens des Europäischen Datenschutzbeauftragten (EDSB) in seiner Entscheidung vom 5. Jänner 2022, GZ: 2020-1013, in Bezug auf den Einsatz von Google Analytics vertreten.

Im gegenständlichen Fall wurden die im digitalen Fußabdruck enthaltenen Informationen – so auch die Google-Analytics Kennnummer – an die Server von Google LLC mit Sitz in den USA übermittelt. Der Betreiber der Webseite und Google LLC haben zwar Standarddatenschutzklauseln (damals noch in der Fassung des Durchführungsbeschlusses der Europäischen Kommission 2010/87/EU vom 5. Februar 2010) abgeschlossen. Ausgehend von der Rechtsprechung des EuGH in C-311/18 („Schrems II“) wurde diese Datenübermittlung als unzulässig beurteilt, weil kein angemessenes Schutzniveau für die übermittelten personenbezogenen Daten, wie gemäß Art. 44 DSGVO gefordert, gegeben war.

Die zusätzlich zu den Standarddatenschutzklauseln implementierten Maßnahmen („supplementary measures“) waren aus Sicht der Datenschutzbehörde nicht effektiv, da diese die seitens des EuGH aufgezeigten Überwachungs- und Zugriffsmöglichkeiten durch US-Behörden nicht erfasst haben. Die Frage der seitens Google LLC angebotenen „IP-Anonymisierungsfunktion“ spielte hingegen keine Rolle, da diese fallbezogen nicht genutzt wurde. Zur Vollständigkeit ist aber festzuhalten, dass IP-Adressen (immer) zunächst vollständig übertragen und erst anschließend in einem zweiten Schritt maskiert werden. Mit anderen Worten: Es kommt zumindest kurzfristig jedenfalls zur Verarbeitung der vollständigen IP-Adresse auf einem Server von Google LLC.

Im Ergebnis hat die Datenschutzbehörde mit Bescheid festgestellt, dass Webseiten-Betreiber das Tool Google Analytics (jedenfalls auf Grundlage des im Bescheid festgestellten Sachverhalts) nicht in Einklang mit Kapitel V der DSGVO einsetzen können.

Der nicht rechtskräftige Bescheid ist in pseudonymisierter Form auf der Webseite der Datenschutzbehörde abrufbar.

„Impfbeschwerden“

Im November bzw. Dezember 2021 wurden in Österreich persönlich adressierte Schreiben im Zusammenhang mit Informationen betreffend COVID-19 und SARS-CoV-2 versandt. Während ein Schreiben, welches vom Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz verschickt wurde, sich an bereits geimpfte Personen richtete und über die Wichtigkeit des Abschlusses der Grundimmunisierung informierte, richteten sich die anderen Schreiben, welche vom Dachverband der Sozialversicherungsträger sowie von den Bundesländern Vorarlberg, Wien und Tirol verschickt wurden, an ungeimpfte Personen und informierten über das Risiko schwer an COVID-19 zu erkranken und die Möglichkeit der Inanspruchnahme einer kostenlosen Impfung gegen SARS-CoV-2.

Im Zusammenhang mit den versandten Impf-Schreiben sind bei der Datenschutzbehörde insgesamt 4.890 Beschwerden eingegangen. Der Großteil der Beschwerdeführerinnen und Beschwerdeführer erachtete sich durch das Impf-Schreiben im Recht auf Geheimhaltung als verletzt und führte hierzu erklärend aus, dass dem Schreiben eine unzulässige Verarbeitung ihrer personenbezogenen Daten zugrunde liegen würde.

Aufgrund dieses enormen Beschwerdeanfalls – im Vergleich dazu langten im Jahr 2019 bei der Datenschutzbehörde insgesamt 2.102 Beschwerden und im Jahr 2020 1.603 Beschwerden ein – wurde in der Datenschutzbehörde eine eigene Task-Force, bestehend aus zehn Bediensteten, eingerichtet.

Im Rahmen des Ermittlungsverfahrens zeigte sich, dass für die Ermittlung der Adressaten der Impf-Schreiben zunächst der jeweilige Impfstatus im zentralen Impfregister abgefragt und dieser anschließend mit Daten des zentralen Patientenindex zur Erhebung der aktuellen Wohnadresse abgeglichen wurde.

Die Datenschutzbehörde gelangte in ihren Verfahren gegen den Dachverband der Sozialversicherungsträger zur Ansicht, dass sich dieser hinsichtlich der oben beschriebenen Datenverarbeitung auf die Bestimmung des § 750 ASVG stützen konnte und wies die Beschwerden entsprechend ab.

In den Verfahren gegen den Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz, das Amt der Vorarlberger Landesregierung und das Amt der Tiroler Landesregierung kam die Datenschutzbehörde hingegen zur Ansicht, dass sich die Verantwortlichen auf keine entsprechende gesetzliche Grundlage stützen konnten und gab den Beschwerden daher statt.

Die Bescheide der Datenschutzbehörde betreffend den Dachverband der Sozialversicherungsträger sind mit Ausnahme von vier Bescheiden in Rechtskraft erwachsen. Die Bescheide der Datenschutzbehörde betreffend den Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz (mit Ausnahme von einem Bescheid), das Amt der Vorarlberger Landesregierung und das Amt der Tiroler Landesregierung sind im Berichtszeitraum nicht in Rechtskraft erwachsen.

Im Berichtszeitraum konnten von Seiten der Datenschutzbehörde die Beschwerden gegen den Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz, den Dachverband der Sozialversicherungsträger sowie das Land Tirol und das Land Vorarlberg betreffend die behauptete Verletzung im Recht auf Geheimhaltung, sohin 3.550 Verfahren, bescheidmäßig abgeschlossen werden. Bei den übrigen Verfahren ist mit einem Abschluss im Jahr 2023 zu rechnen.

3.2.1.2 Grenzüberschreitende Fälle der DSB⁵

Im Jahr 2022 wurden bei der DSB 236 Beschwerdefälle eingebracht, die einen grenzüberschreitenden Sachverhalt iSd Art. 4 Z 23 DSGVO aufwiesen. In 374 Fällen wurde die DSB als mögliche federführende iSd Art. 56 Abs. 1 DSGVO oder betroffene Aufsichtsbehörde iSd Art. 4 Z 22 lit. a und b DSGVO von anderen Aufsichtsbehörden kontaktiert.

Eine bei der DSB eingebrachte Beschwerde mündete etwa in einem verbindlichen Beschluss des Europäischen Datenschutzausschusses über die von der irischen Aufsichtsbehörde vorgelegte Streitsache betreffend Meta Platforms Ireland Limited und ihres Facebook-Dienstes (3/2022, 5. Dezember 2022)⁶. Als betroffene Aufsichtsbehörde aufgrund der Beschwerdeerhebung hatte die DSB neben anderen Aufsichtsbehörden einen maßgeblichen und begründeten Einspruch iSd Art. 4 Z 24 DSGVO erhoben. Im Rahmen des Beschlusses des Europäischen Datenschutzausschusses wurde die irische Aufsichtsbehörde zur Änderung ihres Entscheidungsentwurfs dahingehend aufgefordert, dass ein Verstoß gegen Art. 6 Abs. 1 DSGVO und den Grundsatz von Treu und Glauben gemäß Art. 5 Abs. 1 lit. a DSGVO festzustellen sei, da sich Meta Platforms Ireland Limited im Zusammenhang mit den Nutzungsbedingungen von Facebook nicht auf einen Vertrag als Rechtsgrundlage für die Verarbeitung personenbezogener Daten zum Zweck personalisierter Werbung berufen könne, weil dies kein Kernelement der Dienste sei. Zudem wurde die irische Aufsichtsbehörde angewiesen Meta Platforms Ireland Limited aufzutragen, die Verarbeitung personenbezogener Daten für personalisierte Werbung im Rahmen der Dienste von Facebook innerhalb von drei Monaten in Einklang mit den Bestimmungen der DSGVO zu bringen. Im Hinblick auf einen möglichen Verstoß gegen die Pflichten des Verantwortlichen bei der Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DSGVO wies der Europäischen Datenschutzausschuss die irische Aufsichtsbehörde an, eine Untersuchung durchzuführen. Als Folge des Beschlusses des Europäischen Datenschutzausschusses, wonach für die zusätzlichen Verstöße gegen Artikel 6 Abs. 1 DSGVO sowie gegen die Transparenzverpflichtungen eine Geldbuße auszusprechen sei, um den Erfordernissen der Wirksamkeit, Verhältnismäßigkeit und Abschreckung zu entsprechen, verhängte die irische Aufsichtsbehörde gegen Meta Platforms Ireland Limited in ihrer endgültigen Entscheidung zu Facebook eine Geldbuße in Höhe von 210 Millionen Euro.

Die DSB war seit 25. Mai 2018 bis Ende 2022 in 93 Verfahren als federführende Aufsichtsbehörde gegenüber einem Verantwortlichen tätig, wobei den anderen betroffenen Aufsichtsbehörden iSd Art. 4 Z 22 DSGVO seitens der DSB im Jahr 2022 in 14 Verfahren ein Beschlussentwurf gemäß Art. 60 Abs. 3 DSGVO vorgelegt wurde. Davon wurden 13 Verfahren mit einer gütlichen Einigung beendet, da die behauptete Rechtsverletzung im Laufe des Verfahrens nachträglich beseitigt wurde.

Im Jahr 2022 sind der DSB 15 Sicherheitsverletzungen gemeldet worden, die einen grenzüberschreitenden Sachverhalt aufgewiesen haben. In 20 Fällen betreffend Sicherheitsverletzungen wurde die DSB als mögliche federführende iSd Art. 56 Abs. 1 DSGVO oder betroffene Aufsichtsbehörde iSd Art. 4 Z 22 lit. a und b DSGVO von anderen Aufsichtsbehörden kontaktiert.

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 Siehe hierzu auch Kapitel 6.1.1.

Im Rahmen der grenzüberschreitenden Zusammenarbeit innerhalb und außerhalb eines konkreten Verfahrens machte die DSB im Jahr 2022 155 Mal von der gegenseitigen Amtshilfe iSd Art. 61 DSGVO Gebrauch und wurde selbst in 442 Fällen von anderen Aufsichtsbehörden kontaktiert.

Insgesamt wurden seit dem 25. Mai 2018 bis Ende 2022 von allen Aufsichtsbehörden 512 Beschlussentwürfe iSd Art. 60 Abs. 3 DSGVO vorgelegt und 143 finale Beschlüsse iSd Art. 60 Abs. 6 DSGVO getroffen.⁷

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 und FAQ zum Thema Datenschutz und Cookies

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

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 zu dem Auslaufen der Standardvertragsklauseln, zum Thema Abmahnungen wegen Google Fonts und Informationen über die Entscheidung der Datenschutzbehörde über die Verwendung von Google Analytics.

Darüber hinaus finden sich auf der Webseite der Datenschutzbehörde ausführliche Informationen über die Rechte der betroffenen Personen und die Zuständigkeit der Datenschutzbehörde. Der Leitfaden zur DSGVO wird laufend aktualisiert. Ebenso sind FAQ zum Thema Cookies und Datenschutz auf der Website der Datenschutzbehörde zu finden.

FAQ zum Thema Datenschutz und Cookies

Die Datenschutzbehörde hat FAQ zum Thema Datenschutz und Cookies auf ihrer Webseite (Menüpunkt: „Download & Links“) veröffentlicht. In den FAQ wird auf praxisrelevante Fragen eingegangen, wie zum Beispiel die Gestaltung eines Cookie-Banners, die Zulässigkeit des Modells „pay or okay“ oder unter welchen Voraussetzungen eine Einwilligung für das Setzen und Auslesen von Cookies erforderlich ist. Die FAQ wurden in „nicht juristischer“ Sprache geschrieben, damit das Thema auch für Laien verständlich ist. Die FAQ werden laufend ergänzt. In weiterer Folge werden die wichtigsten Punkte der FAQ erläutert.

⁷ 137 finale Beschlüsse gemäß Art. 60 Abs. 7 DSGVO (Stattgabe der Beschwerde), 5 finale Beschlüsse gemäß Art. 60 Abs. 8 DSGVO (Abweisung oder Ablehnung der Beschwerde) und ein finaler Beschluss gemäß Art. 60 abs. 9 DSGVO (Beschwerde wird zum Teil stattgegeben und zum Teil abgewiesen oder abgelehnt).

Man versteht unter Cookies kleine Textdateien, die am Endgerät – also etwa am Computer oder Smartphone – bzw. im Browser abgespeichert werden, wenn eine Webseite im Internetbrowser aufgerufen wird. Diese Textdateien können u.a. vom Webserver einer solchen Webseite ausgelesen werden. Wird etwa eine Webseite in fünf verschiedenen Sprachversionen angeboten und wird beim erstmaligen Aufruf der Webseite die Sprachversion „Deutsch“ ausgewählt, so wird am Endgerät nun eine Textdatei („Cookie“) samt der Information hinterlegt, dass die Webseite in der deutschen Sprache angezeigt werden soll. Wenn die Cookies nicht gelöscht werden und wenn die Webseite mit demselben Browser erneut aufgerufen wird, so weiß die Webseite aufgrund des hinterlegten Cookies, dass die Webseite in deutscher Sprache angezeigt werden soll.

Aus rechtlicher Sicht ist beim Setzen oder Auslesen von Cookies Art. 5 Abs. 3 der Richtlinie 2002/58/EG idgF. zu beachten, welcher auf nationaler Ebene in § 165 Abs. 3 TKG 2021 umgesetzt wurde. Zusammengefasst dürfen Cookies beim Aufruf einer Webseite nur dann ohne Einwilligung gesetzt oder ausgelesen werden, wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Nutzer oder Benutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann („technisch notwendige Cookies“). Für alle „technisch nicht notwendigen Cookies“ muss daher eine Einwilligung eingeholt werden. Die Bedingungen für eine solche Einwilligung richten sich nach Art. 4 Z 11 und Art. 7 DSGVO. In den FAQ sind Beispiele zu finden, wann aus Sicht der Datenschutzbehörde von einer „technischen Notwendigkeit“ von Cookies auszugehen ist.

Auf nationaler Ebene obliegt der Vollzug eines Verstoßes gegen § 165 Abs. 3 TKG 2021 grundsätzlich dem Fernmeldebüro. Eine Zuständigkeit der Datenschutzbehörde kann aber gegeben sein, wenn als Folge des Einsatzes von Cookies personenbezogene Daten gemäß Art. 4 Z 1 DSGVO verarbeitet werden. Dies kann insbesondere bei sog. „Tracking-Cookies“ der Fall sein, die das Surfverhalten von Nutzern aufzeichnen, um in Folge personalisierte Werbung anzuzeigen. Es gilt zu beachten, dass derartige Aufzeichnungen in manchen Fällen auch mit einem Profil auf einer Social Media Plattform in Verbindung gebracht werden können.

In der Praxis stellt sich oft die Frage, wie ein Cookie-Banner (also die Schaltfläche, mit welcher die Einwilligung eingeholt wird) rechtskonform gestaltet sein muss. In den FAQ sind Handlungsempfehlungen für die Gestaltung eines Cookie-Banners vorhanden. Die Datenschutzbehörde vertritt insbesondere den Standpunkt, dass die Nichtabgabe einer Einwilligung (bzw. das Weitersurfen ohne Einwilligung) genauso einfach sein muss wie die Abgabe der Einwilligung. Mit anderen Worten: Für die Nichtabgabe einer Einwilligung dürfen nicht mehr Interaktionen mit dem Cookie-Banner notwendig sein, als für die Abgabe der Einwilligung. Von der betroffenen Person kann nicht verlangt werden, dass sie auf einer Schaltfläche erst auf einer zweiten oder dritten Ebene die Entscheidung treffen kann, keine Einwilligung abzugeben. Darüber hinaus dürfen betroffene Personen weder unmittelbar noch subtil zur Abgabe einer Einwilligung gedrängt werden (kein „nudging“). Es entspricht keiner fairen Praxis, den Button zur Nichtabgabe einer Einwilligung (bzw. zum Weitersurfen ohne Einwilligung) derart zu gestalten oder zu positionieren, dass dieser Button weniger prominent ist, als der Button zur Abgabe einer Einwilligung.

Schließlich widmen sich die FAQ auch der Frage, ob eine „Cookiewall“ zulässig ist. Bei einer solchen „Cookiewall“ kann für den Zutritt zur Webseite entweder Geld bezahlt werden, alternativ kann die Einwilligung für den Einsatz von Cookies (üblicherweise zum Ausspielen von personalisierter Werbung) abgegeben werden. Umgangssprachlich bezeichnet man dies auch als „pay or okay“. Die Datenschutzbehörde hat in der Vergangenheit mit Bescheid vom 20. August 2019, GZ: DSB-D122.974/0001-DSB/2019, bereits ausgesprochen, dass ein derartiges Modell grundsätzlich zulässig sein kann. Zwar gibt es zu dieser Frage noch keine Judikatur des EuGH,

allerdings spricht für die Entscheidung der Datenschutzbehörde, dass offenbar auch der europäische Gesetzgeber davon ausgeht, dass personenbezogene Daten – zumindest im gewissen Ausmaß – für den Erhalt einer Leistung bereitgestellt werden können (vgl. die Richtlinie (EU) 2019/770 idgF.). In den FAQ sind Anforderungen zu finden, die bei „pay or okay“ jedenfalls zu beachten sind.

Zwischenzeitig hat auch der Europäische Datenschutzausschuss (EDSA) einen Bericht zum Thema Datenschutz und Cookies veröffentlicht („Report of the work undertaken by the Cookie Banner Taskforce, adopted on 17 January 2023“). Der Report kann auf der Website des EDSA heruntergeladen werden. Die darin enthaltenen Ausführungen decken sich im Wesentlichen mit den FAQ der Datenschutzbehörde.

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 Angemessenheitsbeschluss⁸ der Europäischen Kommission besteht, sieht Art. 46 DSGVO unterschiedliche rechtliche Instrumente zur Sicherstellung eines angemessenen Datenschutzniveaus⁹ vor.

Grundsätzlich ist eine Genehmigung dieser Instrumente durch die zuständige Aufsichtsbehörde nur mehr in bestimmten Fällen gemäß Art. 46 Abs. 3 DSGVO vorgesehen. Dies ist etwa bei Bestimmungen in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen gemäß Art. 46 Abs. 3 lit. b DSGVO der Fall. Im Rahmen eines solchen Genehmigungsprozesses ist gemäß Art. 46 Abs. 4 iVm. Art. 63 ff DSGVO auch der Europäische Datenschutzausschuss zu befassen.

Eine weitere Ausnahme bilden die sog. „Verbindlichen internen Datenschutzhinrichten“¹⁰ (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 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 – zum Teil über mehrere Jahre – erstrecken. Es sollte daher vorab immer nach der Notwendigkeit von BCRs gefragt und abgewogen werden, ob die Zulässigkeit der Datenübermittlung nicht einfacher und effizienter

8 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.

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

10 Art. 46 Abs. 2 lit. b iVm. Art. 47 DSGVO. Zu beachten ist, dass BCRs ausschließlich als Übermittlungsinstrument für gruppeninterne Datentransfers herangezogen werden können.

11 Detaillierte Erläuterungen zu den materiellen Voraussetzungen von BCRs sind den Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules des Europäischen Datenschutzausschusses (bis Jänner 2023 in öffentlicher Begutachtung) sowie dem Working Document on Binding Corporate Rules for Processors, WP257/rev.01 der ehemaligen Artikel-29-Datenschutzgruppe 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>; der finale BCR-Entwurf muss dem Europäischen Datenschutzausschuss iSd. Art. 64 Abs. 1 lit. f DSGVO zwingend zur Stellungnahme vorgelegt werden.

durch andere geeignete Garantien iSd. Art. 46 Abs. 2 DSGVO, wie etwa durch die modularen Standarddatenschutzklauseln der Europäischen Kommission¹³, 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.¹⁴

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.¹⁵ Auch in diesen Fällen ist eine Befassung des Europäischen Datenschutzausschusses sowie der Europäischen Kommission vorgesehen.¹⁶

Bei der Datenschutzbehörde wurde im Jahr 2022 ein neues Genehmigungsverfahren nach Art. 46 Abs. 3 lit. b DSGVO anhängig gemacht und positiv behandelt. Zwei in den Vorjahren anhängig gemachte Verfahren zur Genehmigung von verbindlichen internen Datenschutzvorschriften nach Art. 47 DSGVO wurden im Berichtszeitraum aufgrund einer Zurückziehung der zugrundeliegenden Anträge eingestellt.

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 2022

Die Datenschutzbehörde hat im Jahr 2022 17 Bescheide im Rahmen der §§ 7 und 8 DSG erlassen – davon fünf Zurückweisungen. Mit Ausnahme eines Antrages betreffend die Zurverfügungstellung von Adressen hatten die Bescheide Genehmigungen von Verarbeitungen personenbezogener Daten für im öffentlichen Interesse liegende Archiv-, wissenschaftliche, historische oder statistische Zwecke zum Gegenstand. Thematisch wurden (Bild)-Datenverarbeitungen zur Erforschung des autonomen Fahrens im Straßenverkehr, Datenverarbeitungen im Zusammenhang mit historischen Recherchen zu NS-Strafgefangenen oder auch Datenverarbeitungen betreffend die bildbasierte Analyse von Personensammlungen an öffentlichen Orten behandelt.

13 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.

14 Vgl. hierzu das Arbeitsdokument WP74 der ehemaligen Artikel-29-Datenschutzgruppe, abrufbar in deutscher Sprache unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_de.pdf

15 Art. 40 Abs. 3 bzw. Art. 42 Abs. 2 DSGVO; siehe hierzu *Europäischer Datenschutzausschuss*, Leitlinien 4/2021 über Verhaltensregeln als Instrument für Übermittlungen, Fassung 2.0, abrufbar in deutscher Sprache unter https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_codes_conduct_transfers_after_public_consultation_de.pdf; sowie ders, Guidelines 07/2022 on certification as a tool for transfers, Version 1.0 (derzeit in weiterer Überarbeitung), abrufbar in englischer Sprache unter https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf.

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

Hinsichtlich § 7 Abs. 3 DSG ist der Bescheid der Datenschutzbehörde vom 20. Mai 2022 zur VZ D202.303 (GZ 2022-0.283.829) hervorzuheben, mit dem einem Antrag für die Erstellung einer Studie für den Zweck der Erforschung zukünftiger Anforderungen an Stromnetze Folge gegeben worden ist. Konkret wurde die dafür notwendige Verarbeitung personenbezogener Daten der Endverbraucher zum Zustand von Stromnetzen und dem aktuellen Energiebedarf in Form des Verbrauchertyps, der Anschluss- und Erzeugungsleistung, der Zuordnung zu einem entsprechenden Netzknoten sowie der Last- bzw. Erzeugungsprofile von Lastprofilzählern (zeitlich in 15- Minuten-Schritten aufgelöst) genehmigt. Der Antrag erfüllte sämtliche Voraussetzungen des § 7 Abs. 3 DSG. Erstens erfüllte die Antragstellerin als anerkannte Forschungseinrichtung das Kriterium des Art. 7 Abs. 3 Z 3 DSG. Zweitens war das Kriterium des öffentlichen Interesses iSv. Art. 7 Abs. 3 Z 2 DSG aufgrund des gegenständlichen Forschungsprojektes vorliegend. Schließlich war das Kriterium des Art. 7 Abs. 3 Z 1 DSG deswegen gegeben, weil der potentielle Kreis der betroffenen Personen im Vorhinein unbekannt war und eine Ausforschung ihrer Kontaktdaten nur mit einem unverhältnismäßig hohen Aufwand möglich war.

Mit dem Bescheid vom 14. Dezember 2022 zur VZ D202.319 (GZ 2022-0.798.454) wurde einem Antrag auf Erteilung einer Genehmigung gem. § 8 Abs. 3 und Abs. 4 DSG stattgegeben. Verfahrensgegenständlich ging es um die Ermittlung von Adressen von 200 Reha-PatientInnen, die zu einem Stichtag die kardiologische Reha-Phase II abgeschlossen hatten. Nach Selektion anhand bestimmter Kriterien in ihrer Krankenakte sollte ihnen an die eruierten Adressen einmalig ein Fragbogen zwecks Durchführung einer Studie einer außeruniversitären Forschungsorganisation zugesendet werden. Insbesondere die vorherige Einholung der Einwilligung der 200 PatientInnen, nur um ihnen danach die Fragebögen zu übermitteln, hätte einen unverhältnismäßigen Aufwand dargestellt.

3.2.5 Amtswegige Prüfverfahren

Die DSB hat im Jahr 2022 190 amtswegige Verfahren eingeleitet; 133 amtswegige Verfahren wurden im Berichtszeitraum einer Enderledigung (Bescheid oder Einstellung) zugeführt.

Ausgewählte Entscheidungen:

1. Bescheid vom 1. März 2022, GZ: D213.971, 2022-0.021.739

Die Datenschutzbehörde hat in diesem Bescheid festgehalten, dass die Verantwortliche gegen die DSGVO verstoßen hat, indem sie personenbezogene Daten von Dienstnehmern mittels eines in Dienstfahrzeugen eingebauten GPS-Systems verarbeitet hat. Der Verantwortlichen wurde mit sofortiger Wirkung untersagt, die mit dem GPS-Systems ermittelten personenbezogene Daten zu verarbeiten.

Die Verantwortliche hat in fünfzehn Firmenfahrzeuge GPS-Tracker einbauen lassen. Das GPS-System wurde zunächst lediglich zur konkreten Abfrage nach dem Fahrzeugstandort genutzt. Später wurde das System zur Zeiterfassung und für die Diätenabrechnung sowie als Fahrtenbuch erweitert.

Im Rahmen einer Interessenabwägung kam die Datenschutzbehörde zum Ergebnis, dass es an der Erforderlichkeit der Datenverarbeitung mangelt, weshalb eine Berufung auf Art. 6 Abs. 1 lit. f DSGVO ausscheidet.

Die Verantwortliche stützte die Datenverarbeitung des Weiteren auf Bestimmungen des Arbeitszeitgesetzes (AZG) und prüfte die Datenschutzbehörde daher auch, ob die Bestimmungen

des AZG eine rechtliche Verpflichtung zur Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. c DSGVO durch ein GPS-System begründen.

Im Summe erwies sich die Datenverarbeitung auf Basis von Art. 6 Abs. 1 lit. c DSGVO schon deshalb als unzulässig, weil der Zweck auch durch gelindere Mittel, welche eine geringere Datenverarbeitung mit sich bringen (Art. 5 Abs. 1 lit. c), erreicht werden hätte können.

Dieser Bescheid ist nicht rechtskräftig.

2. Bescheid vom 22. April 2022, GZ: D213.1503, 2022-0.016.020

In diesem Verfahren ist die Datenschutzbehörde zum Ergebnis gekommen, dass die Verantwortliche (eine politische Partei) gegen die DSGVO verstoßen hat, indem sie personenbezogene Daten unrechtmäßig durch die Versendungen von Emails in einem offenen E-Mail-Verteiler offengelegt hat und dadurch politische Meinungen der Betroffenen mangels Erlaubnistatbestands gem. Art 9 Abs. 2 DSGVO unrechtmäßig verarbeitet hat.

Die Verantwortliche versendete zwei E-Mails mit einem offenen Verteiler, welcher ca. 400 – zum Teil personalisierte und private – E-Mail-Adressen beinhaltete. Im Anhang der E-Mail befanden sich Schreiben mit politischem Inhalt.

Die Datenschutzbehörde hielt in ihren rechtlichen Erwägungen fest, dass die personenbezogenen E-Mail-Adressen als Daten besonderer Kategorie iSv. Art. 9 DSGVO zu qualifizieren sind, da sie eine politische Meinung zum Ausdruck bringen, welche den betroffenen Inhabern der gegenständlichen Emailadressen vonseiten der Verantwortlichen im Kontext zu den versendeten Schreiben zugeschrieben wurde. Es ist dabei unbedeutlich, ob sich die politischen Meinungen der Betroffenen tatsächlich mit denen, die ihr vonseiten der Verantwortlichen zugeschrieben wurde, exakt decken oder nicht.

Im vorliegenden Fall war keine Ausnahme des Verarbeitungsverbotes von besonderen Kategorien personenbezogener Daten iSd Art. 9 Abs. 2 DSGVO einschlägig und hat die Verantwortliche die Daten der betroffenen Personen daher unrechtmäßig verarbeitet.

Dieser Bescheid ist rechtskräftig.

3. Bescheid vom 30. Mai 2022, GZ: D213.1560, 2022-0.286.157

In diesem Verfahren hat sich die Datenschutzbehörde mit der Frage auseinandergesetzt, ob Mitglieder eines Dienststellausschusses Daten des Personalverzeichnisses verwenden dürfen, um postalische Werbeschreiben für den Beitritt zu einer Gewerkschaft zu versenden.

Die Datenschutzbehörde hat ein amtsweigiges Prüfverfahren gegen zwei Mitglieder eines Dienststellausschusses (als Verantwortliche) eingeleitet. Diese haben gemäß § 9 Abs. 3 lit. i Bundes-Personalvertretungsgesetz (PVG) zur Erfüllung ihrer Aufgaben Zugriff auf das Personalverzeichnis sowie die darin enthaltenen Daten der Bediensteten. Im gegenständlichen Fall wurden diese Daten seitens der Verantwortlichen verwendet, um für den Beitritt zu einer Gewerkschaft zu werben.

Es wurde festgestellt, dass eine derartige Datenverarbeitung keine Deckung im PVG findet und daher unrechtmäßig war. Dies ergibt sich aus einem Vergleich mit Rechtsgrundlagen, die für andere - gesetzliche - Interessenvertretungen gelten: So ist etwa in § 17a Arbeiterkammergesetz (AKG) die ausdrückliche Erlaubnis der Verwendung personenbezogener Daten der Arbeiterkammer-Mitglieder für (Wahl)Werbung vorsehen. Eine entsprechende Regelung für die

Wirtschaftskammer findet sich in § 86 Abs. 3 Wirtschaftskamergesetz (WKG). Die Schaffung einer gesetzlichen Grundlage zur - wie der hier erfolgten - Datenverarbeitung zwecks Anwerbung als Gewerkschaftsmitglied obliegt dem Gesetzgeber. Vor diesem Hintergrund waren die Verantwortlichen gemäß Art. 58 Abs. 1 lit. d DSGVO auf diesen Verstoß hinzuweisen, damit das Verhalten nicht wiederholt wird und um die Verantwortlichen gemäß Art. 57 Abs. 1 lit. d DSGVO für ihre datenschutzrechtlichen Pflichten zu sensibilisieren.

Dieser Bescheid ist rechtskräftig.

3.2.6 Beschwerdeverfahren vor dem Bundesverwaltungsgericht einschließlich Säumnisbeschwerden

Gegen Straferkenntnisse, Verwarnungen und sonstige Bescheide der Datenschutzbehörde besteht die Möglichkeit, eine Beschwerde zu erheben. Das Bundesverwaltungsgericht ist für die Beschwerden gegen Bescheide der Datenschutzbehörde zuständig. 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).

Im Jahr 2022 wurden 1.156 Beschwerden gegen Bescheide der Datenschutzbehörde erhoben.

Es gab 37 Säumnisbeschwerden im Berichtszeitraum.

Ausgewählte Entscheidungen:

W214 2234934-1/24E, Erkenntnis 13. Dezember 2022

Die Datenschutzbehörde leitete ein amtsweigiges Prüfverfahren (Art. 58 Abs. 2 lit. b DSGVO iVm § 22 DSG) zur Prüfung der Einhaltung der Bestimmungen der DSGVO und des DSG und im Besonderen zur Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten der Teilnehmer eines Kundenbindungsprogrammes gegen den Betreiber eines solchen ein.

Die Datenschutzbehörde sprach nach Beendigung des Verfahrens mit Bescheid vom 30. Juli 2020, GZ: 2020-0. 465. 771, aus, dass die für diese Datenverarbeitung eingeholten Einwilligungen nicht den Anforderungen der Art. 4 Z 11 DGSVO und Art. 7 DSGVO entsprechen und die Datenverarbeitung daher mangels Rechtsgrundlage unrechtmäßig erfolgt sei. Zusätzlich wurde die Datenverarbeitung von der Datenschutzbehörde untersagt.

Das Bundesverwaltungsgericht bestätigte den Bescheid der Datenschutzbehörde aus inhaltlicher Sicht, änderte die Spruchpunkte jedoch in Anbetracht der zwischenzeitlich ergangenen Judikatur des Verwaltungsgerichtshofes zur Feststellungskompetenz in amtsweigigen Prüfverfahren ab. Insbesondere wurde daher die von der Datenschutzbehörde festgestellte Verletzung behoben (siehe dazu auch Punkt 4.3. des Datenschutzberichts).

Die eingeholte Einwilligung der Teilnehmer wurde vom Bundesverwaltungsgericht als unzulässig qualifiziert.

Bei der Beurteilung der Gültigkeit einer Einwilligung muss die Sichtweise eines Durchschnittsverbrauchers herangezogen werden. Ein Unterschriftenfeld, das am Ende einer Anmeldestrecke platziert ist und mit dem eine Einwilligung für Profiling – die gegenständliche Datenverarbeitung entsprach dieser Definition – eingeholt wird, genügt den gesetzlichen Vorgaben nicht. Ein Durchschnittsverbraucher wird annehmen, dass mit der Einwilligung nur die Anmeldung

bestätigt wird, zumal im gegenständlichen Fall nicht hinreichend auf Profiling hingewiesen wurde. Ausschlaggebend ist der Gesamteindruck.

Das Bundesverwaltungsgericht hielt zudem fest, dass sich die Frage der Zulässigkeit von Werbeschreiben per E-Mail zwar nach dem TKG 2021 richtet, die vorgelagerte Datenverarbeitung jedoch nach der DSGVO.

Die Datenverarbeitung des Profiling – vom Bundesverwaltungsgericht gegenständlich als nicht unerheblicher Eingriff in das Grundrecht auf Datenschutz bezeichnet – kann zudem nicht nachträglich auf Art. 6 Abs. 1 lit. b oder lit. f DSGVO gestützt werden, da es sich um Zusatzangebote handelt und auch eine Anmeldung ohne Einwilligung möglich ist.

W258 2239561-1/10E, Erkenntnis vom 22. Juli 2022

Mit diesem Erkenntnis des Bundesverwaltungsgerichtes wurde eine Beschwerde gegen den Bescheid der DSB vom 4. Jänner 2021, GZ: D124.3152, 2020-0.825.300, als unbegründet abgewiesen.

Das Bundesverwaltungsgericht hielt in seiner Entscheidung insbesondere fest, dass ein Schulleiter als Verantwortlicher iSd. Art. 4 Z 7 DSGVO für den Betrieb der Schulwebseite zu qualifizieren ist, weil er über die Veröffentlichung der Daten auf der Webseite der Berufsschule entscheide.

Das Bundesverwaltungsgericht bestätigte die Entscheidung der Datenschutzbehörde und erachtete die Veröffentlichung des Namens und der dienstlichen E-Mail-Adresse des Beschwerdeführers, eines Lehrers einer Berufsschule, auf der Webseite der Berufsschule durch den Beschwerdegegner (der Direktor der Schule) gemäß Art. 6 Abs. 1 lit. e iVm Abs. 3 lit. b DSGVO iVm § 56 Abs. 2 Schulunterrichtsgesetz (SchUHG) für gerechtfertigt. Die Veröffentlichung dieser personenbezogenen Daten ist demnach geeignet, es Schülern und Erziehungsberechtigten im Anlassfall einfach und rasch zu ermöglichen, mit dem jeweiligen Lehrkörper in Kontakt zu treten und verringert zudem den Verwaltungsaufwand für die Schule selbst. Auch eine Verletzung der allgemeinen Verarbeitungsgrundsätze des Art. 5 DSGVO wurde vom Bundesverwaltungsgericht nicht festgestellt.

Das Bundesverwaltungsgericht sprach jedoch aus, dass eine Revision zulässig ist, weil es an Rechtsprechung des Verwaltungsgerichtshofes fehle, ob bei der Prüfung des Grundsatzes der Datenminimierung zu prüfen ist, ob eine mögliche Datenminimierung für den Verantwortlichen zumutbar ist, und welchen Anforderungen eine solche Zumutbarkeitsprüfung genügen muss. Überdies fehle es an Rechtsprechung des Verwaltungsgerichtshofes, ob § 56 SchUHG eine Rechtsgrundlage iSd. Art. 6 Abs. 1 lit. e bzw. Abs. 3 lit. b DSGVO darstelle.

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

W256 2236773-1/7E, Erkenntnis vom 8. September 2022

Das Bundesverwaltungsgericht bestätigte mit diesem Erkenntnis erstmalig, dass sogenannte Dash-Cams unter bestimmten Voraussetzungen datenschutzrechtlich zulässig sein können. Das Bundesverwaltungsgericht hat die Beschwerde abgewiesen und die Revision für unzulässig erklärt.

Die Datenschutzbehörde hatte eine Beschwerde bezüglich einer anlassbezogenen (gefährliches Fahrverhalten eines anderen Verkehrsteilnehmers) 2-minütigen Aufzeichnung per Dash-Cam

und der Übermittlung an eine Strafverfolgungsbehörde abgewiesen, weil die Datenverarbeitung nach Ansicht der Datenschutzbehörde im Rahmen des Art. 6 Abs. 1 lit. f DSGVO gedeckt und nicht überschließend war.

Das Bundesverwaltungsgericht hat in seinem Erkenntnis den Bescheid und die darin getätigten Ausführungen bestätigt und festgehalten, dass die Nutzung einer Dash-Cam zulässig sein kann. So kann dem Erkenntnis des Verwaltungsgerichtshofs vom 12. September 2016, Ro 2015/04/0011, nicht entnommen werden, dass die Nutzung einer Dash-Cam generell unzulässig ist, sondern ist jeweils eine Einzelfallbeurteilung erforderlich.

Im Rahmen der Interessenabwägung ist aber jedenfalls entscheidend, dass es sich um eine Nutzung im Rahmen eines konkreten Anlassfalles handelt und keine – in Anbetracht des Zweckes – überschließende Verarbeitung stattfindet. Schon der Verdacht einer strafrechtlichen Handlung stellte aber grundsätzlich ein (allgemeines) berechtigtes Interesse an der Aufklärung dar.

Dieses Erkenntnis ist rechtskräftig.

W108 2246273-1/10E, Erkenntnis vom 30. Mai 2022

Die Datenschutzbehörde hatte sich in Folge der medial als „Postskandal“ bezeichneten Datenverarbeitung durch die Verantwortliche in zahlreichen Fällen mit der Frage auseinanderzusetzen, ob die Verarbeitung der aus der Sozialforschung stammenden „Sinus-Geo Milieus“ in den Anwendungsbereich des Art. 9 DSGVO fällt. Die gegenständlichen Daten stellen statistisch errechnete Wahrscheinlichkeitswerte dar, die Betroffenen zugeschrieben wurden, um diesen gezielt Werbung übermitteln zu können. Folgende Begriffe samt Übereinstimmung ausdrückender Prozentpunkte wurden den betroffenen Personen zugeordnet: Konservative, Traditionelle, Etablierte, Performer, Postmaterielle, Digitale Individualisten, Bürgerliche Mitte, Adaptiv Pragmatische, Konsumorientierte Basis, Hedonisten.

Das Bundesverwaltungsgericht bestätigte, dass aus diesen Zuschreibungen vermeintliche weltanschauliche Überzeugungen der Betroffenen hervorgehen und es sich bei diesen Angaben sohin um Daten besonderer Kategorie im Sinne des Art. 9 Abs. 1 DSGVO handelt.

Das Bundesverwaltungsgericht führte diesbezüglich außerdem aus, dass es unerheblich ist, dass die Verantwortliche die Daten von einer Dritten bezogen hatte, da sie diese in weiterer Folge in ihrer eigenen Datenbank verarbeitete.

Dieses Erkenntnis wurde mit Revision bekämpft und vom Verwaltungsgerichtshof wegen Rechtswidrigkeit infolge Verletzung von Verfahrensvorschriften – Unterlassung einer mündlichen Verhandlung – aufgehoben.

W256 2226003-1/5E, Erkenntnis vom 8. März 2022

Ein Beschwerdeführer hatte die Berichtigung eines Bescheids des BMI in einer Entschädigungssache gemäß § 8 Polizeibefugnis-Entschädigungsgesetz verlangt und diesbezüglich Beschwerde bei der Datenschutzbehörde eingebracht. Berichtigt werden sollten alle Passagen der Begründung, die auf die gegen den Beschwerdeführer im Zeitpunkt der Amtshandlung bestehende Verdachtslage Bezug nahmen, zumindest im Umfang einer Ergänzung seiner Einwände, sowie sein falsch geschriebener bzw. abgekürzter akademischer Grad.

Gegen den Bescheid des BMI war kein Rechtsmittel, jedoch eine Neuaufrollung vor Gericht (Klage gemäß § 9 Polizeibefugnis-Entschädigungsgesetz) zulässig.

Das Bundesverwaltungsgericht hat mit seinem Erkenntnis vom 8. März 2022 die Beschwerdeabweisung durch die Datenschutzbehörde (Bescheid vom 11. Oktober 2019, GZ: DSB-D124.1456/0003-DSB/2019) bestätigt. Einleitend hielt das Bundesverwaltungsgericht fest, dass der Beschwerdeführer seinen Berichtigungsantrag fälschlicherweise hauptsächlich auf § 45 DSG gestützt hatte, eine Entschädigungssache gemäß § 8 Polizeibefugnis-Entschädigungsgesetz fällt jedoch in den Anwendungsbereich der DSGVO. In der Hauptsache stellte das Bundesverwaltungsgericht unter Berufung u.a. auf die analoge Anwendung des Urteiles des EuGH vom 17. Juli 2014, Rs C-141/12 und C-372/12, YS ua., klar, dass die Berichtigung des Textes einer behördlichen Entscheidung (über die in § 68 AVG eingeräumten Möglichkeiten hinaus) nicht auf Art. 16 DSGVO gestützt werden kann.

Dieses Erkenntnis ist rechtskräftig.

3.2.6a Beschwerdeverfahren vor dem Bundesverwaltungsgericht in Verwaltungsstrafsachen der Datenschutzbehörde

Im Berichtszeitraum wurden **zwei Beschwerden gegen Straferkenntnisse** der Datenschutzbehörde erhoben. Darüber hinaus wurde **ein Verfahrenshilfeantrag** gestellt, um eine Beschwerde gegen ein Straferkenntnis der Datenschutzbehörde einzubringen. Es wurden **keine Beschwerden gegen Verwarnungen**, die von der Datenschutzbehörde im Berichtszeitraum ausgesprochen wurden, eingebracht¹⁷.

Die geringe Anzahl an Beschwerden im Berichtszeitraum ist darauf zurückzuführen, dass die überwiegende Anzahl an Entscheidungen der Datenschutzbehörde in Verwaltungsstrafsachen (Verwarnungen, Straferkenntnisse) mangels Erhebung eines Rechtsmittels in Rechtskraft erwuchsen.

Zudem hat die Datenschutzbehörde im Berichtszeitraum keine Straferkenntnisse oder Verwarnungen gegenüber juristischen Personen ausgesprochen, da anhängige Verfahren gegen juristische Personen bis zur Entscheidung des EuGH iS C-807/21 (Deutsche Wohnen) mittels Bescheid ausgesetzt wurden.¹⁸ Es gab im Berichtszeitraum in diesem Zusammenhang **eine Beschwerde gegen einen diesbezüglichen Aussetzungsbescheid** der Datenschutzbehörde.

Zu den anhängigen Beschwerdeverfahren beim Bundesverwaltungsgericht im Zusammenhang mit der Strafbarkeit von juristischen Personen nach Art. 83 DSGVO

Die Datenschutzbehörde hat im Jahr 2021 (bis zum Vorabentscheidungsverfahren des EuGH iS C-807/21, Deutsche Wohnen) mehrere Straferkenntnisse gegenüber juristischen Personen erlassen¹⁹ und eine Zurechnung iSd § 30 Abs. 1 und 2 DSG vorgenommen. Durch das Vorabentscheidungsverfahren beim EuGH zu C-807/21 stellte sich jedoch die Frage, ob solche Voraussetzungen, wie z.B. in § 30 Abs. 1 und 2 DSG normiert, für die Strafbarkeit von juristischen Personen gegen Unionsrecht (konkret gegen Art. 83 DSGVO) verstoßen und daher nicht zur Anwendung gelangen dürfen.

Darüber hinaus wird im Vorabentscheidungsverfahren die Frage geklärt, ob eine Geldbuße gegen ein Unternehmen iSd Art. 4 Z 18 DSGVO nur dann verhängt werden kann, wenn der Verstoß gegen die DSGVO vorsätzlich oder fahrlässig begangen worden ist oder ob Geldbußen aufgrund

17 Im Kapitel 3.2.10 befindet sich eine Statistik zu den verhängten Geldbußen und Verwarnungen der Datenschutzbehörde im Berichtszeitraum.

18 Siehe Datenschutzbericht 2021, 3.2.10 S. 50.

19 Siehe Datenschutzbericht 2021, 3.2.10 S. 49 ff (demonstrative Aufzählung)

einer verschuldensunabhängigen Haftung verhängt werden können, da dies in Art. 83 DSGVO nicht ausdrücklich normiert ist.

Bis zur Einleitung des Vorabentscheidungsverfahrens iSD C-807/21 hat die Datenschutzbehörde in ihren Straferkenntnissen gegen juristische Personen eine Zurechnung iSD § 30 Abs. 1 und 2 DSG sowie iSD Judikatur des Verwaltungsgerichtshofs zur Strafbarkeit juristischer Personen²⁰ vorgenommen. Die Datenschutzbehörde hat daher im Spruch konkret angeführt, dass eine identifizierte bzw. namentlich genannte natürliche (Führungs-)Person eine bestimmte Handlung vornahm (oder eine solche unterließ) und rechnete der juristischen Person das tatbestandsmäßige, rechtswidrige und schuldhafte Verhalten der natürlichen Person im Spruch zu. Den Zurechnungspersonen wurde von der Datenschutzbehörde auch eine Parteistellung im Sinne eines Beschuldigten eingeräumt, da ihre Handlung bzw. Unterlassung der juristischen Person in Folge zugerechnet wurde. Diese - über die in Art. 83 DSGVO hinausgehenden und strengereren - Voraussetzungen waren nach Ansicht des Verwaltungsgerichtshofs für die Verhängung einer Geldbuße über eine juristische Person nach der österreichischen Rechtslage erforderlich.

Die Beschwerdeführer (juristische Personen) haben in Folge im Rahmen ihrer Beschwerden gegen die Straferkenntnisse unter anderem die konkret von der Datenschutzbehörde im Spruch vorgenommene Zurechnung sowie das von der Datenschutzbehörde als erwiesen angenommene Verschulden moniert, da - ihrer Ansicht nach - die herangezogenen Zurechnungspersonen weder iSD § 30 Abs. 1 DSG selbst den vorgeworfenen Verstoß begangen noch iSD § 30 Abs. 2 DSG eine Aufsichts- oder Sorgfaltspflicht verletzt haben.

Die Entscheidung des EuGH im genannten Vorabentscheidungsverfahren hat somit präjudizelle Wirkung für die anhängigen Beschwerdeverfahren. Die Entscheidung des EuGH hat nicht nur Auswirkungen auf die konkrete Gestaltung des Spruchs der Straferkenntnisse²¹, sondern auch darauf, wie Verwaltungsstrafverfahren gegen juristische Personen pro futuro von der Datenschutzbehörde zu führen sein werden²².

Das Bundesverwaltungsgericht hat daher den überwiegenden Teil anhängiger Beschwerdeverfahren in Verwaltungsstrafsachen gegen juristische Personen bis zur Entscheidung des EuGH ausgesetzt²³. Auch der Verwaltungsgerichtshof setzte ein Amtsrevisionsverfahren in Verwaltungsstrafsachen mit Bezug auf die Strafbarkeit juristischer Personen aus²⁴. Nur in einem Fall setzte das Bundesverwaltungsgericht das Beschwerdeverfahren nicht aus und bestätigte das Straferkenntnis der Datenschutzbehörde dem Grunde nach (siehe unten im Detail).

Erkenntnis des Bundesverwaltungsgerichts vom 14.07.2022, W274 2245288-1

Das Bundesverwaltungsgericht hat mit gegenständlichem Erkenntnis einer Beschwerde einer juristischen Person gegen ein Straferkenntnis der Datenschutzbehörde teilweise Folge gegeben und die Strafe reduziert. Die Beschwerde wurde ansonsten als unbegründet abgewiesen und das Straferkenntnis der Datenschutzbehörde dem Grunde nach bestätigt. Die Entscheidung des Bundesverwaltungsgerichts erging trotz Hinweis der Datenschutzbehörde auf das beim EuGH anhängige Vorabentscheidungsverfahren C-807/21 (siehe oben).

20 Vgl VwGH 12.05.2020, Ro 2019/04/0229.

21 Beschuldigte haben ein subjektives Recht darauf, dass ein Straferkenntnis den in § 44a Z 1- 5 VStG festgelegten Erfordernissen in Bezug auf den Spruch des Bescheides entspricht, vgl. VwGH 26. 1. 2012, 2010/07/0011.

22 Vgl. BVwG 08.04.2022, W214 2243436-1.

23 Vgl beispielsweise BVwG 25.05.2022, W176 2249328-1; BVwG 08.04.2022, W214 2243436-1; BVwG 31.03.2022, W256 2246230-1.

24 Vgl VwGH 24.02.2022, Ra 2020/04/0187.

Im konkreten Fall verhängte die Datenschutzbehörde eine Geldbuße in der Höhe von insgesamt EUR 8.000,- (zusätzlich EUR 800,- Verfahrenskosten) gegenüber einer juristischen Person (GmbH) wegen unrechtmäßiger Verarbeitung personenbezogener (Bild-)Daten durch den Betrieb einer Videoüberwachungsanlage außerhalb eines Geschäftslokals sowie wegen Verstoßes gegen die Informationspflicht gemäß Art. 13 DSGVO, da die Betroffenen nicht über die Verarbeitung im Aufnahmebereich iSd Art. 12 und 13 DSGVO informiert wurden.

Das Bundesverwaltungsgericht hat den Schuldausspruch bestätigt, jedoch die Strafe auf EUR 5.000,- reduziert. Der Begründung zufolge war eine Aussetzung des Verfahrens bis zur Entscheidung des EuGH in der oben genannten Vorabentscheidungssache nicht erforderlich, da die Datenschutzbehörde die Zurechnung iSd § 30 Abs. 1 und 2 DSG sowie iSd Judikatur des Verwaltungsgerichtshofs zur Strafbarkeit juristischer Personen²⁵ korrekt vornahm. Selbst wenn der EuGH die Voraussetzung einer Zurechnung iSd § 30 DSG als unionsrechtswidrig bewertet, würde sich nichts am Tatvorwurf gegen die juristische Person ändern.

Darüber hinaus bestätigte das Bundesverwaltungsgericht die von der Datenschutzbehörde im Rahmen von Art. 6 Abs. 1 lit. f DSGVO durchgeführte Interessenabwägung und führte ins Treffen, dass die Verarbeitung wegen des Aufnahmebereichs (weit überschließender Aufnahmebereich öffentlicher Verkehrsflächen) und der eingestellten Speicherdauer von 4 Wochen nicht auf berechtigte Interessen gestützt werden konnte.

In Bezug auf das Vorbringen der Beschwerdeführerin, wonach aus der DSGVO keine Kennzeichnungspflicht einer Videoüberwachungsanlage zu entnehmen sei, führte das Bundesverwaltungsgericht aus, dass es dem europäischen Datenschutzrecht bereits lange innewohne, dass Betroffene über eine Bildaufnahme informiert sein müssen. Nur dann können Betroffene auch ihre Rechte nach der DSGVO gegenüber dem Verantwortlichen ausüben. Ein Verantwortlicher müsse in diesem Zusammenhang seiner Informationspflicht gemäß Art. 13 DSGVO jedenfalls nachkommen.

Mit Verweis auf die Leitlinien des Europäischen Datenschutzausschusses²⁶ vertrat das Bundesverwaltungsgericht die Ansicht, dass aufgrund der Informationsmenge ein „geschichteter Zugang“ gewählt werden kann, um der Informationspflicht zu entsprechen. Die wichtigsten Informationen sollten in einem Warnhinweis dargestellt werden (erste Schicht), während die restlichen Informationen mit anderen Mitteln zur Verfügung gestellt werden (zweite Schicht).

Der Umstand einer allfälligen Sichtbarkeit der Kameras kann das Erfordernis einer geeigneten Kennzeichnung keinesfalls kompensieren. Im Zusammenhang mit der Frage nach der ausreichenden Bestimmtheit der Strafnorm nach Art. 5 Abs. 1 lit. a iVm Art. 12 und 13 iVm Art. 83 Abs. 1 und 5 lit. a DSGVO hatte das Bundesverwaltungsgericht keine Zweifel.

In Bezug auf die subjektive Tatseite führte das Bundesverwaltungsgericht aus, dass es dem Geschäftsführer der Beschwerdeführerin jedenfalls zumutbar war, sich vor Inbetriebnahme der Anlage über die Rechtslage zu informieren. Aufgrund der mangelnden Erkundigung konnte daher auch kein Verbotsirrtum angenommen werden. Der Geschäftsführer handelte insgesamt objektiv sorgfaltswidrig und sein schuldhaftes Verhalten wurde der beschuldigten juristischen Person zugerechnet.

25 Vgl VwGH 12.05.2020, Ro 2019/04/0229.

26 Vgl Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, S. 21 f.

Hinsichtlich der Strafbemessung bestätigte das Bundesverwaltungsgericht zunächst die Entscheidung der Datenschutzbehörde, statt einer Verwarnung eine Geldbuße auszusprechen, da im konkreten Fall von keinem geringfügigen Verstoß gegen die DSGVO ausgegangen werden konnte und insbesondere im Sinne der Generalprävention eine Geldbuße erforderlich war. Lediglich in Bezug auf die Strafhöhe schloss sich das Bundesverwaltungsgericht der Beschwerdeführerin an und reduzierte die Strafe, da in einem vergleichbaren Fall einer Videoüberwachung öffentlicher Verkehrsflächen eine Geldbuße in der Höhe von EUR 4.800,- verhängt worden war.²⁷ Das Erkenntnis des Bundesverwaltungsgerichts erwuchs in Rechtskraft.

Erkenntnis des Bundesverwaltungsgerichts vom 25.10.2022, W256 2222862-1

Der Beschwerde eines KFZ-Halters gegen ein Straferkenntnis der Datenschutzbehörde aus dem Jahr 2019, in welchem eine Geldstrafe in der Höhe von EUR 500,- wegen der unrechtmäßigen Nutzung einer Dash-Cam-Anlage (Armaturenbrett-Videokamera) verhängt worden war, wurde vom Bundesverwaltungsgericht Folge gegeben und das Verwaltungsstrafverfahren eingestellt. Die Revision gemäß Art. 133 Abs. 4 B-VG wurde für nicht zulässig erklärt.

Das Gericht begründete seine Entscheidung damit, dass die Bildverarbeitung im öffentlichen Raum mittels einer Dash-Cam-Anlage nicht per se als unzulässig bewertet werden kann, sondern im Rahmen einer Einzelfallbeurteilung überprüft werden muss, indem eine Interessenabwägung vorgenommen wird. Das Bundesverwaltungsgericht kam im konkreten Fall zum Ergebnis, dass die Verarbeitung im Tatzeitraum (im Zuge eines Verkehrsdelikts) durch die verfahrensgegenständliche Dash-Cam-Anlage aufgrund von Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen des Verantwortlichen) gerechtfertigt war, da im vorliegenden Sachverhalt eine Auswertung aufgrund eines Anlassfalles (Verkehrsdelikt) erfolgt ist und das Bildmaterial zur Ausforschung des Verursachers des Verkehrsunfalls herangezogen wurde (ähnlich: BVwG 08.09.2022, W256 2236773-1, siehe Kapitel 3.2.6). Dass bereits drei Minuten vor dem Anlassfall Bildmaterial aufgezeichnet wurde (bzw. dieses im verwendeten Ringspeicher nicht mehr überschrieben wurde), sah das Gericht als nicht unverhältnismäßig an. Dies auch, obwohl der Fahrer durch das Herausziehen der Speicherkarte die Überschreibung der Bilddaten nach eigenem Gutdünken gestoppt hatte.

Es wird darauf hingewiesen, dass das Bundesverwaltungsgericht die Verarbeitung ausschließlich zum Zeitpunkt des Verkehrsdeliktes und nicht den generellen Betrieb der Dash-Cam-Anlage beurteilte. Zu diesem Zeitpunkt hatte der Beschwerdeführer wegen einer Kollision mit einem anderen KFZ die Speicherkarte aus seiner Dash-Cam-Anlage gezogen und dadurch eine Bildaufnahme in der Dauer von drei Minuten erstellt. Daher sei der konkrete Fall bzw. die Zulässigkeit der Verarbeitung aufgrund eines konkreten Anlassfalles zu beurteilen (anders als der Verwaltungsgerichtshof in seiner bisherigen Rechtsprechung zum Betrieb von Dash-Cam-Anlagen per se).²⁸ Eine außerhalb der Tatzeit (konkret außerhalb des Verkehrsdeliktes) allenfalls erfolgte darüberhinausgehende Verarbeitung personenbezogener Daten sei nicht vom Tatvorwurf umfasst und somit nicht Gegenstand des Verfahrens.

Die Entscheidung ist rechtskräftig.

Erkenntnis des Bundesverwaltungsgerichts vom 13.12.2022, W252 2247268-1

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

27 Vgl DSB 12.09.2018, D550.038/0003-DSB/2018.

28 Vgl. VwGH 12.09.2016, Ro 2015/04/0011.

Im konkreten Fall verhängte die Datenschutzbehörde eine Geldbuße gegenüber einer natürlichen Person in der Höhe von EUR 600,- wegen unrechtmäßiger Bildverarbeitung durch eine Videoüberwachungsanlage sowie wegen Verstoßes gegen die Informationspflicht nach Art. 13 DSGVO. Der Beschwerdeführer betrieb eine Videoüberwachungsanlage, die auf ein Nachbargrundstück und auf einen Teilbereich einer öffentlichen Gemeindestraße gerichtet war (Aufnahmebereich). Das Bundesverwaltungsgericht folgte überwiegend der Ansicht der Datenschutzbehörde, nahm jedoch für einen Teil des Tatzeitraums Fahrlässigkeit und keinen Vorsatz an. Daher wurde die Strafe auf EUR 400,- reduziert.

Das Bundesverwaltungsgericht führte darüber hinaus zum Begriff „*personenbezogene Daten*“ aus, dass die vom Beschwerdeführer vorgebrachte „*schlechte Auflösung*“ der Kamera nicht zum Ergebnis führt, dass keine personenbezogenen Daten im Tatzeitraum verarbeitet wurden. Der Beschwerdeführer konnte seinen Nachbarn persönlich und konnte durch die Verknüpfung von Informationen mit den Bilddaten eine Identifizierung vornehmen. Dadurch war eine indirekte Identifizierung der Betroffenen möglich.

Das Gericht führte zudem ins Treffen, dass selbst die Information darüber, ob der Nachbar des Beschwerdeführers gerade zuhause war und wie lange dieser wach war (anhand des brennenden Lichts im Haus sei dies erkennbar gewesen) unter dem Begriff „*personenbezogene Daten*“ zu subsumieren sei, da sich daraus Informationen über die Lebensgewohnheiten der Betroffenen ableiten lassen.

Das Bundesverwaltungsgericht führte eine Interessenabwägung durch und kam zum Ergebnis, dass die Verarbeitung jedenfalls in der konkreten Form nicht erforderlich war. Zweck der Kamera war der Schutz von Eigentum während der Abwesenheit des Beschwerdeführers im Sommer. Der Beschwerdeführer hätte einen anderen Kamerawinkel wählen müssen und zwar selbst wenn dies allenfalls mit Hürden (Stromversorgung, WLAN-Empfang) verbunden gewesen wäre. Die Erfassung des Grundstücks der Nachbarn war jedenfalls für den Zweck nicht erforderlich. Das Gericht führte schließlich als Alternative ins Treffen, dass physische Blenden oder das Verpixeln nicht relevanter Bereiche ebenfalls zumutbar waren.

In Bezug auf die subjektive Tatseite führte das Gericht aus, dass der Beschwerdeführer einem vorwerfbaren Verbotsirrtum für einen Teil des Tatzeitraum unterlag, da er gegen seine Erkundigungspflicht verstieß. Hierzu führte das Gericht ins Treffen, dass es dem Beschwerdeführer bekannt sein musste, dass es einschlägige Datenschutzvorschriften gibt, da über die DSGVO seit 2018 breit in der Öffentlichkeit informiert und diskutiert wurde, eine große Anzahl medialer Beiträge zu diesem Thema erschienen sind und Datenschutz durch die Digitalisierung ein ständiger Begleiter ist. Als der Beschwerdeführer jedoch von seinem Nachbarn auf die Kamera angesprochen wurde und sich trotzdem weigerte, den Winkel zu ändern, handelte er mit Vorsatz (dolus eventualis).

Das Gericht folgte dem Beschwerdeführer lediglich in Bezug auf die Strafhöhe und reduzierte die Strafe, weil nicht für den gesamten Tatzeitraum Vorsatz angenommen werden konnte. Das Erkenntnis ist nicht rechtskräftig.

3.2.7 Verfahren über die Meldung der Verletzung des Schutzes personenbezogener Daten

Im Berichtsjahr wurden der Datenschutzbehörde 818 nationale Sicherheitsverletzungen („Data Breaches“) gemäß Art. 33 DSGVO gemeldet.

Dazu kamen 15 Meldungen betreffend grenzüberschreitender Sicherheitsverletzungen sowie 20 Sicherheitsverletzungen, die an andere Aufsichtsbehörden im Unionsgebiet herangetragen und der Datenschutzbehörde aufgrund von potentieller Betroffenheit iSd Art. 4 Abs. 22 DSGVO im Rahmen eines Verfahrens gemäß Art. 65 DSGVO zur Kenntnis gebracht wurden.

Von Betreibern öffentlicher Kommunikationsdienste wurden 25 Sicherheitsverletzungen nach § 164 TKG 2021 (vormals § 95a TKG 2003) 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.

Im Jahr 2022 ist es wieder zu einem verstärkten Aufkommen - im Vergleich zum Berichtsjahr 2021 - der gemeldeten Vorfälle, die in Verbindung mit unterschiedlichsten Arten von Ransomware standen, gekommen, wobei bei diesen Angriffen zumeist eine Verschlüsselung von Daten das Ziel gewesen zu sein schien, mitunter kam es je nach benutzter Software auch zur Übermittlung der Daten an die Angreifer (Hacker). Zumeist reicht dem Angreifer eine Verschlüsselung der Daten aus, ohne dass die Daten nach außen übertragen werden. Gegen eine geldwerte Gegenleistung entschlüsselt dieser wieder die Daten.

Auch ist es gehäuft zur Übertragung von Schadsoftware auf das System des Verantwortlichen durch die Öffnung von E-Mail-Anlagen gekommen, welche in weiterer Folge E-Mails (zum Teil mitsamt dem vorherigen Schriftverkehr mit dem jeweiligen Verantwortlichen) an gespeicherte bzw. zuvor verwendete E-Mail-Adressen weiterleiteten. Darüber hinaus lagen auch Ransomware ähnliche Angriffe vor, bei denen der Verantwortliche Dienste über das Internet anbietet und von Dritten (Hackern) Schwachstellen ausgenutzt worden sind.

In den oben genannten Fällen ist rasches Handeln geboten sowie die Einleitung von Maßnahmen, die zur Reduzierung des Risikos führen. Dies kann beispielsweise das Herunterfahren der mit Schadsoftware kompromittierten Server, das Löschen der Schadsoftware, die Abänderung der Passwörter, das Heranziehen eines IT-Forensikers, die genaue Analyse bzw. Auswertung, wie es zu diesem Vorfall kommen konnte und wie derartiges in Zukunft vermieden werden kann, sein.

Hintergrund der Regelung des Art. 33 DSGVO ist, dass eine Verletzung einen Schaden – wie beispielsweise der Verlust der Kontrolle über personenbezogene Daten, die Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder Betrug, finanzielle Verluste oder die unbefugte Aufhebung der Pseudonymisierung - für natürliche Personen nach sich ziehen kann, sofern keine rechtzeitige und angemessene Reaktion erfolgt. Aus diesem Grund trifft den Verantwortlichen die Pflicht, die Risiken für die Rechte und Freiheiten der betroffenen Person zu bewerten und geeignete technische und organisatorische Maßnahmen zu ergreifen, um diese hintanzuhalten. Zudem sollten die Maßnahmen dem aktuellen Stand der Technik entsprechen. Neben dem Element der Datensicherheit obliegt dem Verantwortlichen die Verpflichtung, falls trotz Setzung geeigneter Maßnahmen ein Verstoß eintreten sollte, rechtzeitig zu reagieren und diesen zu melden.

Liegt bei einer Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die betroffenen Personen vor, kann die Datenschutzbehörde daher einen Verantwortlichen entsprechend Art 58 Abs. 2 lit. e DSGVO anweisen, eine nach Art. 34 Abs. 1 DSGVO gebotene Benachrichtigung nachzuholen. Die Datenschutzbehörde kann bei Gefahr im Verzug einen Mandatsbescheid iSd § 22 Abs. 4 DSG erlassen.

Abschließend wird auch in diesem Zusammenhang erwähnt, dass der EDSA die Leitlinien zur Meldung von Verstößen gegen personenbezogene Daten aktualisiert und mit 10. Oktober 2022 angenommen hat (vgl. Guidelines 9/2022 on personal data breach notification under GDPR).

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 2022 wurde die Datenschutzbehörde als Aufsichtsbehörde in drei Fällen gemäß Art. 36 DSGVO konsultiert.

Im Verfahren zur GZ: D485.009 gab die Verantwortliche an, dass sie nach dem COVID-19-Impf-pflichtgesetz (§§ 3b und 6) zur Vornahme von Datenverarbeitungen verpflichtet werde. Die von der Verantwortlichen vorgebrachten Bedenken betrafen im Wesentlichen die Rechtsgrundlage der vorgesehenen Datenverarbeitung iSd Art. 6 Abs. 1 lit. c DSGVO bzw. Art. 9 Abs. 2 lit. i DSGVO im Hinblick auf deren befürchtete Verfassungs- bzw. Unionsrechtswidrigkeit. Die Verantwortliche brachte vor, die COVID-19-Impflicht sei nicht verhältnismäßig, was dazu führe, dass auch die nach dem Gesetz vorgesehenen Datenverarbeitungen nicht verhältnismäßig und damit unzulässig seien. Der Antrag wurde mit Bescheid vom 21. April 2022 zur GZ: 2022-0.263.348 zurückgewiesen, da die behauptete Verfassungs- oder Unionsrechtswidrigkeit eines Gesetzes nicht Gegenstand eines Konsultationsverfahrens nach Art. 36 DSGVO sein kann. Die Befugnisse einer Aufsichtsbehörde nach Art. 36 Abs. 2 iVm Art. 58 DSGVO zielen darauf ab, faktisch Einfluss auf die Datenverarbeitung nehmen zu können. Darüber hinaus obliege die Kompetenz, über die Verfassungswidrigkeit eines Gesetzes zu entscheiden, nicht der Aufsichtsbehörde, sondern gemäß Art. 140 B-VG allein dem Verfassungsgerichtshof.

Der Bescheid ist rechtskräftig, das BwG hat mittlerweile das Beschwerdeverfahren wegen Klaglosstellung eingestellt.

Im Verfahren zur GZ: D485.008 beabsichtigte die Verantwortliche an einem Torbogen (Schwibbogen) ein Videokamerasystem zu montieren, welches mit einem Lichtschranken verbunden ist. Sobald vom durchfahrenden LKW die Fahrzeughöhe von 2,6 Meter überschritten wird, löse

der Lichtschranken aus und aktiviere die beiden Kameras. Das geplante Videokamerasystem erfasse weder Fußgänger noch Personenkraftfahrzeuge, weil diese den Lichtschranken nicht auslösen können. Die Verantwortliche unterließ es, ein hohes Risiko für potentiell betroffene Personen aufzuzeigen, bzw. zu konkretisieren.

Die Datenschutzbehörde wies den Antrag mit Bescheid vom 10. Mai 2022 zur GZ: 2022-0.312.949 zurück, da es nicht Gegenstand eines Verfahrens gemäß Art. 36 DSGVO ist, eine Bestätigung der Datenschutzbehörde zu bekommen, dass die getroffenen Maßnahmen tatsächlich als geeignet anzusehen sind, um die identifizierten Risiken einzudämmen. Eine solche Einschätzung der getroffenen Abhilfemaßnahmen obliegt allein dem Verantwortlichen selbst und kommt eine Konsultation der Datenschutzbehörde nach Art. 36 DSGVO nur in jenen Fällen zur Anwendung, in denen es dem Verantwortlichen nicht gelingt, die ermittelten Risiken hinreichend einzudämmen.

Im Verfahren zur GZ: D485.011 beabsichtigte die Verantwortliche die Anbringung von Videokameras an Bahnstationen der Verantwortlichen. Die Verantwortliche führte aus, dass ein hohes Risiko in Bezug auf die Erteilung der zuverlässigen Information an die betroffenen Personen über die Datenverarbeitung dahingehend gegeben sei, dass es sich bei den Bahnhofstationen um für jedermann zu jeder Zeit öffentlich zugängliche Bereiche handle, was zum Verlust der Vertraulichkeit bzw. zur Geheimnisoffenbarung führen könne. Daher werde das Risiko als hoch eingestuft. Darüber hinaus könne es bei Meldung an das Sicherheitssystem und Einsicht in die Videoaufzeichnungen durch entsprechende Irrannahmen über allenfalls verdächtige Personen zur Rufschädigung oder auch zu finanziellen oder wirtschaftlichen Nachteilen führen, weshalb das Risiko ebenfalls als hoch eingestuft werde.

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.

Demnach soll die Information erster Ebene durch ein aussagekräftiges Hinweisschild erfolgen. Diese Informationen sollten so angebracht sein, dass die betroffene Person die Umstände der Überwachung leicht erkennen kann, bevor sie den überwachten Bereich betritt (etwa in Augenhöhe). Die Position der Kamera selbst muss nicht offengelegt werden, solange kein Zweifel daran besteht, welche Bereiche erfasst werden und die Umstände der Überwachung eindeutig beschrieben werden. Die betroffene Person muss in der Lage sein, einzuschätzen, welcher Bereich von einer Kamera erfasst wird, damit sie der Überwachung ausweichen oder ihr Verhalten erforderlichenfalls anpassen kann (vgl. dazu Rz 113).

Informationen der zweiten Ebene müssen ebenfalls an einem für die betroffene Person leicht zugänglichen Ort zur Verfügung gestellt werden, z. B. als vollständiges Informationsblatt an einer zentralen Stelle (z. B. Informationsschalter, Empfang oder Kasse) oder auf einem leicht zugänglichen Plakat. Wie bereits erwähnt, muss der Warnhinweis der ersten Ebene eindeutig auf die Informationen der zweiten Ebene verweisen. 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 Informationen müssen jedoch auch auf nicht digitalem Wege leicht verfügbar sein. Es sollte möglich sein, auf die Informationen der zweiten Ebene zuzugreifen, ohne sich in den überwachten Bereich zu begeben, insbesondere wenn die Informationen digital bereitgestellt werden (beispielsweise über einen Link). Ein anderes geeignetes Mittel könnte eine Telefonnummer sein, die angerufen werden kann. Die Informationen müssen jedoch alle Angaben enthalten, die nach Art. 13 DSGVO obligatorisch sind (ebd. Rz 117).

Die Verantwortliche sah die Anbringung von Hinweisschildern sowohl beim Bahnsteig am jeweiligen Fahrgastinformationssystem als auch bei vorhandenen Wartehäusern vor. Damit seien die anwesenden Personen bei Betreten der Bahnstationen in der Lage, den Hinweis auf die bei den Bahnstationen vorhandene Videoüberwachung zur Kenntnis zu nehmen; die Hinweisschilder seien vor dem Erfassungsbereich angebracht worden. Außerdem sei am jeweiligen Fahrgastinformationssystem eine eigene „Notrufnummer“ angebracht, welche es auch den betroffenen Personen ermöglicht, den zuständigen Sicherheitsdienst rund um die Uhr zu erreichen. Damit seien die Rechte der betroffenen Personen auf Information, Auskunft, Berichtigung, Löschung etc. im Sinne der DSGVO gewahrt.

Neben der von der Verantwortlichen vorgesehenen Kennzeichnung durch Hinweisschilder seien weitere geeignete Maßnahmen getroffen worden, um das hohe Risiko der betroffenen Personen zu minimieren:

Die Daten der Videoüberwachung seien auf speziell geschützten Servern der Verantwortlichen gespeichert. Die Speicherung der Daten erfolge in verschlüsselter Form und seien zur Verhinderung von Datenverlust entsprechende Firewalls installiert worden und es würden regelmäßige Backups erfolgen. Der dazugehörige Videorekorder sei in der Bahnstation im Schalthaus installiert und es sei in diesem zusätzlich ein eigens verschließbarer Serverschrank montiert worden, damit der physische und elektronische Zugang zu den Daten auf die mit der Projektbearbeitung befassten Personen eingeschränkt sei. Das Schalthaus würde außerdem mit einer Alarmanlage abgesichert werden.

Aufgrund der technischen Einrichtungen würden die erstellten Videoaufzeichnungen nach 72 Stunden durch die Verantwortliche gelöscht. Eine Ausnahme bilde hier der Fall tatsächlich erfolgter rechtswidriger Handlungen, die durch Videoaufzeichnungen dokumentiert seien und der Strafverfolgung oder der Verfolgung oder Verteidigung der Rechte der Verantwortlichen dienen würden. Diese über die 72 Stunden hinausgehende Aufbewahrung erfolge durch ein Vier-Augen-Prinzip. Die Einsichtnahme samt Sicherung sei nur durch die gleichzeitige Anwesenheit zweier Mitarbeiter mit einem jeweils zugehörigen Passwort möglich. Die diesbezüglichen Passwörter seien in separat verschlossenen Kuverts in einem zusätzlich versperrten Schrank verwahrt.

Die Kameraausrichtung erfolge in den Bahnstationen derart, dass nur das Gelände der jeweiligen Bahnstationen erfasst werde, sodass ausgeschlossen sei, dass Bereiche, welche über das jeweilige Gelände der Bahnstationen hinausgehen, erfasst würden.

Die Datenschutzbehörde entschied, dass aufgrund der von der Verantwortlichen in der Datenschutz-Folgenabschätzung vorgenommenen Beurteilung, die Zulässigkeit der gegenständlichen Datenverarbeitung zu bejahen ist und die Datenschutzbehörde hatte der Interessensabwägung der Verantwortlichen nichts entgegenzusetzen.

Darüber hinaus kann aufgrund der von der Verantwortlichen geplanten Aufnahme-, Auswertungs- und Löschmodalitäten das Risiko derart stark reduziert werden, dass im Ergebnis kein hohes Restrisiko für Betroffene erkannt werden kann. Die Verantwortliche hat daher bestehende Risiken hinreichend eingedämmt.

Daher wurde mit Bescheid vom 20. Juni 2022 zur GZ: 2022-0.321.391 der Antrag abgewiesen, da die Voraussetzung für eine vorherige Konsultation gemäß Art. 36 DSGVO mangels hohem Risiko nicht gegeben war

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 neun 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 sechs wurde bereits eine dazugehörige Überwachungsstelle gemäß Art. 41 Abs. 2 DSGVO akkreditiert:

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

Eine Aufzählung findet sich auf der Website der Datenschutzbehörde.²⁹ Darüber hinaus hat auch der Europäische Datenschutzausschuss ein Register von Verhaltensregeln aller Mitgliedstaaten veröffentlicht, welches laufend ergänzt wird.³⁰

Auf der Website der Datenschutzbehörde befindet sich ein „Frage und Antworten“ Bereich zum Thema „Verhaltensregeln und Überwachungsstellen“³¹

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-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 Unter-

29 Verzeichnis gemäß Art. 40 Abs. 6 DSGVO unter [Verzeichnis der genehmigten Verhaltensregeln - Datenschutzbehörde \(dsb.gvat\)](https://www.dsb.gv.at/verzeichnis-der-genehmigten-verhaltensregeln-daten-schutzbehörde-dsb-gvat).

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

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

stützung 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).

Bereits im Dezember 2021 hat die Datenschutzbehörde erstmals ausgesprochen, dass Verhaltensregeln, die faktisch nur für ein Unternehmen gelten würden, nicht genehmigungsfähig sind, da nur Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, Verhaltensregeln ausarbeiten und deren Genehmigung beantragen können (Bescheid vom 9. Dezember 2021, D196.020, 2021-0.857.225, siehe dazu auch den Newsletter 1/2022). Im Jahr 2022 hat die Datenschutzbehörde ihre Spruchpraxis insofern erweitert, als eine Vertretung von Kategorien von Verantwortlichen der betroffenen Branche im Sinne von Art. 42 Abs. 5 DSGVO auch dann nicht gegeben ist, wenn es sich beim Antragsteller um einen Verein mit lediglich zwei Mitgliedern handelt und zwar insbesondere dann, wenn es sich bei diesen zwei Mitgliedern um die Marktführer einer Branche handelt. Diesfalls wird den besonderen Bedürfnissen der kleinen und mittleren Unternehmen einer Branche nicht ausreichend Rechnung getragen (Bescheid vom 13. Dezember 2022, D196.024, GZ: 2022-0.826.387).

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.³²

3.2.10 Verhängung von Geldbußen durch die Österreichische Datenschutzbehörde: Erfahrungs- und Vollzugsbericht 2022

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 2022 bildeten die Verfahren gegen natürliche Personen den größeren Bestandteil der Verwaltungsstrafverfahren.

Die Datenschutzbehörde hat - in diesem Zusammenhang - im Beobachtungszeitraum 28 Geldbußen sowie sieben Verwarnungen ausgesprochen. Insgesamt hat die Datenschutzbehörde im Jahr 2022 Geldbußen in Höhe von knapp über EUR 50.000 verhängt.

Dabei ist zu beachten, dass die Datenschutzbehörde Verwaltungsstrafen im Jahr 2022 lediglich gegenüber natürlichen Personen verhängt hat. Grund dafür ist ein seit dem 21.12.2021 am EuGH anhängiges Vorabentscheidungsverfahren (C-807/21, Deutsche Wohnen), welches sich mit der Frage der Strafbarkeit von juristischen Personen auseinandersetzt (siehe im Detail Punkt 3.2.6a).

Die Datenschutzbehörde hat im Berichtszeitraum zwar Verwaltungsstrafverfahren auch gegen juristische Personen (weiter)geführt und Ermittlungsschritte vorgenommen, hat jedoch aufgrund von entscheidenden Vorfragen (im Zusammenhang mit der Frage der Zurechnung des Verhaltens von natürlichen Personen - insb. Entscheidungsträgern - zur juristischen Person bzw. der Frage des Verschuldens) bis zur Entscheidung des EuGH in zwölf Fällen das jeweilige Verwaltungsstrafverfahren mittels Bescheid gemäß § 38 AVG iVm § 24 VStG ausgesetzt.

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

Darüber hinaus hat die Datenschutzbehörde im Zuge von Verwaltungsstrafverfahren im Berichtszeitraum noch 16 weitere Bescheide (Abweisungsbescheide, Teilzahlungsbescheide, Ladungsbescheide) erlassen.

Hinsichtlich der Anzahl von Verwaltungsstrafverfahren wird auf Punkt 3.1 („Statistische Darstellung“) verwiesen.

Ausgewählte Entscheidungen:

- **Bescheid vom 23. August 2022, D550.509, GZ: 2022-0.585.764 (Unrechtmäßige Bildverarbeitung in einer öffentlichen WC-Anlage)**

Die Verwaltungsstrafverfahren im Zusammenhang mit dem Betrieb einer Bildverarbeitungsanlage bzw. Videoüberwachungsanlage (im Regelfall stationäre Anlagen, die auf Objekten angebracht wurden) bildeten, wie schon die Jahre zuvor, einen wesentlichen Bestandteil der von der Datenschutzbehörde im Jahr 2022 durchgeführten Verwaltungsstrafverfahren.

Es gab jedoch einen Sachverhalt, der aufgrund der Intensität des Eingriffs in das Grundrecht auf Datenschutz von den anderen Fällen deutlich abwich:

Eine natürliche Person (im Folgenden „Beschuldigter“) hat in einem Zeitraum von zwei Monaten an insgesamt drei unterschiedlichen Tagen (für die Dauer von jeweils neun bis zwölf Stunden über den jeweiligen Tag verteilt) in mehreren öffentlich zugänglichen WC-Anlagen an einem Badesee unrechtmäßig und ohne einen legitimen Zweck personenbezogene Daten verarbeitet, indem er innerhalb der Toilettenkabinen eine Bildbearbeitungsanlage in Form einer Mini-WiFi-Kamera versteckt montiert und heimlich betrieben hat. Dadurch zeichnete der Beschuldigte betroffene Personen heimlich bei der Nutzung der WC-Anlage sowie beim Umziehen auf.

Die gegenständliche Verarbeitung konnte auf keinen der in Art. 6 Abs. 1 DSGVO normierten Erlaubnistratbestände gestützt werden und verstieß im Ergebnis gegen mehrere Grundsätze der DSGVO: Art. 5 Abs. 1 lit. a DSGVO („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“), Art. 5 Abs. 1 lit. b DSGVO („Zweckbindung“) sowie Art. 5 Abs. 1 lit. c DSGVO („Datenminimierung“). Darüber hinaus verstieß der Beschuldigte auch gegen seine Informationspflicht nach Art. 13 DSGVO.

Der Sachverhalt wurde zunächst von der Staatsanwaltschaft geprüft und mangels Erfüllung eines (zum Tatzeitpunkt nicht existenten) gerichtlichen Straftatbestandes an die Datenschutzbehörde weitergeleitet. Die Datenschutzbehörde leitete daraufhin ein Verwaltungsstrafverfahren ein. Die Mini-Kamera verfügte über einen Bewegungsmelder und löste eine Aufzeichnung aus, sobald die Kabine von einem Betroffenen betreten wurde. Es konnten vom letzten Einsatz der Kamera ungefähr 600 Video-Dateien sichergestellt werden.

Die Datenschutzbehörde bewertete diesen Eingriff in das Grundrecht auf Geheimhaltung der zahlreichen Betroffenen als äußerst gravierend. Die Betroffenen konnten jedenfalls nicht damit rechnen, dass sie während intimster Momente heimlich von einer Videokamera erfasst und aufgezeichnet werden.

Die Datenschutzbehörde verhängte daher eine Geldbuße in der Höhe von **EUR 25.000,-** (Ersatzfreiheitsstrafe: 336 Stunden, und zusätzliche Verfahrenskosten: EUR 2.500,-).

Das Straferkenntnis wurde rechtskräftig.

- **Bescheid vom 23. September 2022, D550.715, GZ: 2022-0.622.297 (Unrechtmäßiges Facebook-Posting)**

Eine natürliche Person (im Folgenden „Beschuldigte“) hat in einer offenen Facebook-Gruppe intime Details über das Sexualleben einer anderen weiblichen Person („Betroffene“) offengelegt, indem sie im Rahmen eines Beitrages behauptete, dass die Betroffene in Swinger-Clubs unterwegs sei. Es hatte der Beschuldigten missfallen, dass die Betroffene einerseits in Kirchen singt, andererseits in Swinger-Clubs verkehrt, was sie von einem gemeinsamen Bekannten erfahren haben will.

Der betreffende Beitrag war mehrere Stunden online und somit für alle User dieser Facebook-Gruppe zu sehen. Erst auf Aufforderung wurde die Nachricht von der Beschuldigten gelöscht.

Die Verarbeitung der personenbezogenen Daten konnte auf keinen der in Art. 6 Abs. 1 DSGVO normierten Erlaubnistatbestände gestützt werden und verstieß im Ergebnis gegen folgende Grundsätze der DSGVO: Art. 5 Abs. 1 lit. a DSGVO („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“) sowie Art. 5 Abs. 1 lit. c DSGVO („Datenminimierung“).

Die Datenschutzbehörde verhängte eine Geldbuße in der Höhe von **EUR 600,-** (Ersatzfreiheitsstrafe: 36 Stunden).

Die Strafverfügung wurde rechtskräftig.

- **Bescheid vom 5. April 2022, D550.540, GZ: 2022-0.244.681**
- **Bescheid vom 6. April 2022, D550.658, GZ: 2022-0.086.925**
- **Bescheid vom 4. Juli 2022, D550.675, GZ: 2022-0.412.744**
- **Bescheid vom 5. August 2022, D550.628, GZ: 2022-0.467.913**
- **Bescheid vom 12. August 2022, D550.527, GZ: 2022-0.544.376**
- **Bescheid vom 8. September 2022, D550.704, GZ: 2022-0.608.211 (Unrechtmäßige ELGA-Abfragen)**

In sechs Fällen wurden Ärztinnen bzw. Ärzte bzw. ApothekerInnen im vorangegangenen Jahr dafür bestraft, dass sie unrechtmäßig Einsicht in das elektronische Impfregister oder in die ELGA-Gesundheitsakte von betroffenen Personen (MitarbeiterInnen, Familienmitglieder, sonstiger ihnen bekannte Personen) ohne deren Wissen und ohne deren Einwilligung genommen hatten. Die Beweggründe waren zwar unterschiedlich, die Zugriffe konnten jedoch in keinem der Fälle auf einen der in Art. 6 Abs. 1 DSGVO normierten Erlaubnistatbestände gestützt werden und sie verstießen gleich gegen mehrere Grundsätze der DSGVO („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, „Zweckbindung“ sowie „Datenminimierung“).

Die Strafen bewegten sich zumeist bei **mehreren tausend Euro** und wurden in den meisten Fällen rechtskräftig. Darüber hinaus wurden die Ärztekammer bzw. die Apothekerkammer aufgrund gesetzlicher Informationspflichten vom Ausgang der jeweiligen Verwaltungsstrafverfahren benachrichtigt.

- **Bescheid vom 28. Oktober 2022, D550.676, GZ: 2022-0.574.030 [beispielhaft] (Fehlende Kooperation)**

In acht Fällen haben Personen auch im Jahr 2022 nicht auf Aufforderungsschreiben der Datenschutzbehörde (etwa in Beschwerdeverfahren oder in amtsweigigen Prüfverfahren) reagiert und haben so nicht mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammengearbeitet. Diese Personen haben somit gegen Art. 31 DSGVO verstoßen.

Die verhängten Strafen bewegten sich zumeist bei **mehreren hundert Euro**. Bei den Bestraften handelte es sich immer nur um natürliche Personen (siehe den Punkt „Allgemein“ oben).

3.2.11 Stellungnahmen zu Gesetzes- und Verordnungsentwürfen

Die Datenschutzbehörde hat im Jahr 2022 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.

1. Gesetzesentwurf, mit dem das Familienlastenausgleichsgesetz 1967 geändert wird
2. NÖ Hinweisgeberschutzgesetz (NÖ HGSG)
3. Entwurf einer Verordnung der Bundesministerin für Digitalisierung und Wirtschaftsstandort über die Stammzahlenregisterbehörde
4. Entwurf einer Verordnung über das Ergänzungsregister (Ergänzungsregisterverordnung 2022 – ERegV 2022)
5. Entwurf der Universitäts- und Hochschulstatistik- und Bildungsdokumentationsverordnung – UHSBV und Entwurf einer Verordnung, mit der die Studienbeitragsverordnung – StubeiV geändert wird
6. Entwurf einer EAG-Investitionszuschüsseverordnung Strom
7. Entwurf einer Verordnung des Bundesministers für Inneres über die Registrierung und Verwendung eines Elektronischen Identitätsnachweises
8. Entwurf eines Gesetzes, mit dem das Wiener Aufzugsgesetz 2006 (WAZG 2006) geändert wird
9. Transparenzdatenbank-Abfrageverordnung 2022
10. Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung, mit der die Verordnung über die Lehrpläne der Mittelschulen sowie die Verordnung über die Lehrpläne der allgemeinbildenden höheren Schulen geändert werden (Digitale Grundbildung in den Lehrplanbestimmungen)
11. Bundesgesetz, mit dem das Schulorganisationsgesetz, das Schulunterrichtsgesetz, das Schulzeitgesetz 1985 und das Land- und forstwirtschaftliche Bundesschulgesetz geändert werden
12. Änderung des Studienförderungsgesetzes 1992
13. Novelle des Tierschutzgesetzes
14. Änderung der Staatsbürgerschaftsverordnung 1985
15. Ausschussbegutachtung (242/AUA) Parteiengesetz
16. Abgabenänderungsgesetz 2022 (AbgÄG 2022)
17. Klimabonus-Abwicklungsverordnung – KliBAV
18. Novelle der Gewerbeordnung 1994; Neugestaltung der Gewerbelegitimationen
19. Pflegeausbildungs-Zweckzuschussgesetz
20. Bundespflegegeldgesetz
21. HinweisgeberInnenschutzgesetz – HSchG
22. Zweites EU-Informationssysteme-Anpassungsgesetz
23. Erneuerbare-Wärme-Gesetz – EWG
24. Novelle UVP-G
25. Novelle des Wiener Krankenanstaltengesetzes 1987 - Wr. KAG und des Wiener Gesundheitsfonds-Gesetzes 2017
26. TDBG-Novelle 2022
27. Barrierefreiheitsgesetz
28. Verordnungen des BEV, Eichvorschriften für elektrische Tarifgeräte zur Messung von elektrischer Energie an Ladepunkten zum Betrieb von Elektrofahrzeugen
29. Bundesgesetz über die Wiener Zeitung GmbH und Einrichtung einer elektronischen Verlautbarungs- und Informationsplattform des Bundes – WZEVI-Gesetz
30. Entwurf einer Zweiten Transparenzdatenbank-Abfrageverordnung 2022

4 Wesentliche höchstgerichtliche Entscheidungen

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

4.1 Verfahren vor dem Verfassungsgerichtshof

Im Berichtszeitraum sind mehrere datenschutzrechtlich relevante Entscheidungen des Verfassungsgerichtshofes ergangen, wobei die wichtigste und potenziell folgenreichste sicher die Aufhebung des in § 9 Abs. 1 DSG verankerten „Medienprivilegs“ darstellt. Weiters hatte sich der VfGH mit datenschutzrechtlichen Grundrechtsfragen im Umfeld eines Scheidungsverfahrens (Geheimhaltungs- bzw. Auskunftsanspruch betreffend Einkommensdaten und deren Verarbeitung zum Zweck der Errechnung von Unterhaltsansprüchen durch einen Wirtschaftstreuhänder) zu befassen.

Erkenntnis vom 22.9.2022, E 2078/2022

Streitpunkt in dieser Sache war, ob ein Wirtschaftstreuhänder, der im Auftrag einer die Scheidung anstrebenden (Noch-) Ehefrau und mit von letzterer übermittelten Daten eine Bewertung der wirtschaftlichen Kennzahlen einer Privatstiftung und des dem Noch-Ehegatten daraus zufließenden Einkommens zwecks Errechnung möglicher Unterhaltsansprüche durchführte, dadurch den (Noch-) Ehemann im Recht auf Geheimhaltung personenbezogener Daten verletzt hat.

Die DSB hatte die Beschwerde in diesem Punkt abgewiesen, das BVwG hatte diese Entscheidung aufgehoben und der Beschwerde Folge gegeben (Erkenntnis vom 27.6.2022, Zl. W101 2218962-2).

Der VfGH hat dieses Erkenntnis nun wegen Verletzung des Rechts auf Gleichheit vor dem Gesetz (Art. 2 StGG) infolge Willkür bei der Interessenabwägung aufgehoben. Das BVwG verkannte in seiner Entscheidung, dass der (Noch-) Ehemann in der vorliegenden Konstellation gemäß Rechtsprechung des OGH zu Auskunftsansprüchen in Unterhaltsfragen kein Recht auf Geheimhaltung seiner Einkommensdaten hatte. Es besteht insbesondere kein schutzwürdiges Interesse des Unterhaltpflichtigen an der Geheimhaltung seines Einkommens, um sich einer gesetzlichen Unterhaltpflicht zu entziehen.

Erkenntnis vom 22.9.2022, E 2223/2022

Diese Sache schließt sachverhaltsmäßig an das vorige Erkenntnis des Höchstgerichts an, nur dass diesmal das Recht des (Noch-) Ehemanns auf Auskunft über die zu seiner Person verarbeiteten Daten gegenüber dem Wirtschaftstreuhänder Gegenstand der Sache war. Hier hatten DSB und BVwG inhaltlich insoweit gleich entschieden, als der Wirtschaftstreuhänder zumindest verpflichtet gewesen wäre, auf den Auskunftsantrag zu reagieren und eine Verweigerung der inhaltlichen Auskunftserteilung näher zu begründen (Erkenntnis vom 28.7.2022, Zl. W101 2218962-1).

Der VfGH hat auch dieses Erkenntnis nun wegen Verletzung des Rechts auf Gleichheit vor dem Gesetz (Art. 2 StGG) infolge Willkür aufgehoben. Dem Wirtschaftstreuhänder kann es vor dem

Hintergrund seiner berufsrechtlichen Verschwiegenheitspflicht nicht zugemutet werden, eine Handlung zu setzen, welche die Prozessaussichten seiner Auftraggeberin, der (Noch-) Ehefrau, in einem allfälligen Scheidungs- oder Unterhaltsverfahren (potenziell) beeinträchtigen könnte. Der Wirtschaftstreuhänder hat sich somit zu Recht auf seine berufliche Verpflichtung zur Verschwiegenheit gemäß § 80 Abs. 3a WTBG 2017 berufen, ohne dies, anders als vom BVwG angenommen, näher begründen zu müssen.

Erkenntnis vom 14.12.2022, G 287/2022 und G 288/2022

Anlass für dieses Gesetzesprüfungsverfahren waren Beschwerden an die Datenschutzbehörde wegen des Inhalts von Medienberichterstattung (u.a. der Bildaufnahme einer Visitenkarte mit lesbaren Personendaten in einem Bericht über eine Hausdurchsuchung). Die Datenschutzbehörde hatte die Beschwerden unter Anwendung von § 9 Abs. 1 DSG wegen Unzuständigkeit zurückgewiesen.

Gegen die Zurückweisungen erfolgten Bescheidbeschwerden beim BVwG, das daraufhin beim VfGH beantragte, das Medienprivileg als verfassungswidrig aufzuheben (dies zweimal, ein erster Antrag wurde vom VfGH mit Beschluss vom 26.9.2022, G200/2022 ua, wegen zu eng gewählten Umfangs der Anfechtung zurückgewiesen).

§ 9 Abs. 1 DSG sieht in sehr weitem Umfang vor, dass das DSG sowie näher bezeichnete Teile der DSGVO auf journalistische Datenverarbeitungen durch Medien und Medienmitarbeiter nicht anzuwenden sind.

Der VfGH kommt nun zu dem Schluss, dass es dem Grundrecht auf Datenschutz gemäß § 1 DSG widerspricht, Medien prinzipiell in diesem Umfang von der Anwendung des Datenschutzrechts auszuschließen. Es ist nur dann zulässig, durch Gesetz in dieses Grundrecht einzugreifen, wenn der Eingriff zur Wahrung überwiegender berechtigter Interessen eines anderen notwendig ist.

Medien nehmen laut VfGH in einer demokratischen Gesellschaft eine bedeutende Rolle im öffentlichen Interesse wahr („public watchdog“). Die Meinungs- und Informationsfreiheit erfordert daher gemäß Art. 85 DSGVO auch zulässige Ausnahmen, um Datenschutzbestimmungen mit den Besonderheiten der Ausübung journalistischer Tätigkeit vereinbar zu machen. Auch erhöhte Anforderungen an die interne Organisation, Dokumentation und technische Sicherung der Datenverarbeitung durch Medienunternehmen wären laut VfGH möglich.

Das Grundrecht auf Datenschutz erlaubt es jedoch nicht, prinzipiell der Meinungs- und Informationsfreiheit für Tätigkeiten, die zu journalistischen Zwecken ausgeübt werden, den Vorrang vor dem Schutz personenbezogener Daten einzuräumen.

§ 9 Abs. 1 DSG idF BGBl. I Nr. 24/2018 wird daher mit Ablauf des 30. Juni 2024 als verfassungswidrig aufgehoben. Bis dahin ist die Bestimmung, außer in den Anlassfällen, weiterhin anzuwenden. Das heißt, eine Beschwerdeführung gegen Medienunternehmen wegen des Inhalts von Medienberichten ist bis dahin nicht möglich.

Der VfGH deutet an, dass § 9 Abs. 1 DSG in der ursprünglichen, nie Kraft getretenen und noch während der Legisvakanz durch die nunmehr aufgehobene Regelung ersetzen Fassung des Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 120/2017, verfassungskonform sein könnte.

4.2 Oberster Gerichtshof

Der OGH hatte sich im Berichtsjahr vor allem mit Fragen der datenschutzrechtlichen Interessenabwägung im Zusammenhang mit Online-Bewertungssystemen zu befassen, wobei den Interessen der Meinungs- und Informationsfreiheit generell ein sehr hoher Stellenwert eingeräumt worden ist.

Außerdem hatte sich der OGH mit Fragen der Datenverarbeitung (Recht auf Ablehnung) durch digitale Stromzähler (Smart Meter) sowie mit Fragen der Datenverarbeitung für Zwecke der Rechtsdokumentation (Pseudonymisierung von RIS-Entscheidungen) zu befassen.

Weiters hatte er eine Entscheidung zu treffen, durch die die österreichische Rechtslage an ein datenschutzrechtlich relevantes Urteil des EGMR angepasst worden ist (Lückenfüllung durch Gesetzesanalogie).

Urteil vom 2.2.2022, 6 Ob 129/21w

Beklagte waren in dieser Sache der Gründer und wirtschaftliche Eigentümer einer Gesellschaft m.b.H. (Erstbeklagter) und die Gesellschaft selbst (Zweitbeklagte), die eine App zur Bewertung von Lehrern auf den Markt gebracht hatten. Ein Lehrer klagte auf die Unterlassung der Datenverarbeitung und auf Löschung seines Namens und seiner Bewertungen aus der App. Das Gericht erster Instanz wies die Klage ab. Das OLG Wien gab dem Kläger teilweise Recht. Es erlaubte die Datenverarbeitung (die Bewertung und Veröffentlichung) nur, soweit sichergestellt sei, dass der Kläger nur von Personen bewertet wird, die er auch wirklich unterrichtet bzw. unterrichtet hat.

Der OGH hat das abweisende Urteil des Erstgerichts wiederhergestellt. Dies aufgrund einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO zwischen den Grundrechten des Klägers auf Datenschutz und Privatsphäre und dem Grundrecht auf Meinungsausübung und Informationsfreiheit der App-Betreiberin und der App-Nutzer, die zu einem anderen Ergebnis kommt als das OLG Wien. Dabei war ein wichtiger Faktor, dass der Kläger nur hinsichtlich seiner Berufsausübung betroffen ist, weil bei der Berufsausübung ein geringerer Schutz vor öffentlichen Äußerungen besteht als im engeren Bereich der Privatsphäre.

Das Argument der Beklagten, es liege eine Datenverarbeitung für journalistische Zwecke gemäß Art. 85 Abs. 1 DSGVO und § 9 Abs. 1 DSG vor, die unter das Medienprivileg falle, hat der OGH unter Hinweis auf Vorjudikatur des EuGH verworfen. Jedoch sei die Datenverarbeitung in der App vom Grundrecht nach Art 11 GRC geschützt.

Der OGH negiert nicht, dass die für die Datenverarbeitung in der App Verantwortliche gewisse Missbrauchsmöglichkeiten nicht verhindert. Der OGH gewichtet hier die Einschränkung der Rechte des Klägers durch die Missbrauchsmöglichkeit weniger schwer als die Einschränkung der Meinungsausübungsfreiheit, die eintreten würde, wenn sich die Nutzer namentlich registrieren müssten oder wenn eine solche App überhaupt nicht betrieben werden dürfte.

Der OGH betont weiters, dass nur die in diesem Fall durchgeführte Datenverarbeitung (App) beurteilt worden ist.

Beschluss vom 30.3.2022, 8 Ob 3/22g

Mit dieser Entscheidung hat der OGH eine durch das Urteil des EGMR vom 6.4.2021, Appl.5434/17, N*** gegen Österreich, notwendig gewordene Änderung seiner Rechtsprechung in Urkunden- und Grundbuchsfragen vorgenommen.

Nunmehr kann die Ausstellung einer Teilausfertigung eines Scheidungsfolgenvergleichs beantragt werden. Nur diese ist bei der Verbücherung (etwa der Übertragung von Wohnungseigentum) in die Urkundensammlung des Grundbuchs aufzunehmen, sodass dort für Dritte kein vollständiger Einblick in alle anlässlich einer Scheidung getroffenen Regelungen (etwa in Fragen der Obsorge für gemeinsame Kinder) mehr möglich ist. Dies hatte der EGMR als unzulässigen Eingriff in das Recht auf Schutz des Privat- und Familienlebens gemäß Art. 8 EMRK gewertet.

Bisher hatten die Gerichte die Ausstellung einer solchen Teilausfertigung mangels ausdrücklicher gesetzlicher Regelung für nicht zulässig erachtet. Der OGH leitet die Möglichkeit dazu nunmehr aus einer analogen Anwendung von § 178 Abs. 4 AußStrG (Teilausfertigung eines Gerichtsbeschlusses) ab, um die bestehende Gesetzeslücke zu füllen.

Urteil vom 6.4.2022, 6 Ob 36/22w

Gegenstand dieses Verfahrens war eine u.a. auf die DSGVO gestützte Unterlassungsklage eines Strombeziehers, der die Installation eines digitalen Messgerätes („Smart Meter“) an Stelle des elektromechanischen Stromzählers verhindern wollte, gegen eine Netzbetreibergesellschaft (Beklagte). Das Erst- und das Berufungsgericht hatten die Klage abgewiesen.

Auch der (ordentlichen) Revision ist vom OGH nicht Folge gegeben worden.

In dieser ausführlich begründeten Entscheidung kommt der OGH zu dem Schluss, dass mit dem Einbau und der Verwendung der beabsichtigten Messeinrichtung an sich weder eine der DSGVO widersprechende Datenverarbeitung noch eine schwerwiegende Beeinträchtigung der Geheimsphäre (§ 16 ABGB) verbunden ist, die ihren Einbau oder ihre Verwendung unzulässig machen würden. Die Datenverarbeitung kann sich auf den Erlaubnistatbestand gemäß Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) stützen. Es besteht insbesondere die Möglichkeit einer Opt-Out-Konfiguration gemäß § 1 Abs. 6 Intelligente Messgeräte – Einführungsverordnung (IME-VO), in der ein (intelligentes) Messgerät nur die Funktion eines (digitalen) Standardstromzählers erfüllt. Die vom Kläger vorgebrachte bloße Möglichkeit, dass die Beklagte die Einrichtung aus der Ferne umkonfiguriert und damit die Datenverarbeitung ausweitet, spricht nicht gegen den Einbau und die Verwendung dieser Messeinrichtung.

Beschluss vom 27.7.2022, 6 Ob 296/03b

In dieser Sache hat der OGH auf Einschreiten der betroffenen Person von Amts wegen die Frage geprüft, ob eine OGH-Entscheidung in einem Sachwalterschaftsverfahren (nunmehr: Erwachsenenschutzverfahren) wegen überwiegender Interessen der betroffenen Person aus der RIS-Entscheidungsdokumentation der Justiz zu entfernen ist.

Der OGH kam zu dem Schluss, dass die betroffene Person aufgrund der erfolgten Pseudonymisierung des Familiennamens und der Häufigkeit des Vornamens nicht einfach wiedererkannt werden kann. Gemäß § 15 Abs. 1 OGHD sind in die Entscheidungsdokumentation Justiz des RIS alle Entscheidungen des Obersten Gerichtshofs im Volltext aufzunehmen, die sich nicht in einer begründungslosen Zurückweisung eines Rechtsmittels erschöpfen. Das Unterbleiben der Veröffentlichung ist nach der Systematik des Gesetzes eine im Ermessen des erkennenden Senats stehende Ausnahme. Hier würden trotz der Nichtöffentlichkeit des Sachwalterschaftsverfahrens keine ausreichenden Gründe dafür vorliegen, die Entscheidung aus dem RIS zu entfernen.

Beschluss vom 28.7.2022, 11 Ns 59/22y

In dieser Sache hat der OGH entschieden, dass eine Person, die sich auf das Vorliegen einer Verwechslungsgefahr berufen hatte, aber nicht mit der eigentlich betroffenen Person (nicht namensgleicher Verurteilter in einem Finanzstrafverfahren) identisch ist, nicht berechtigt ist,

einen auf Datenschutzrecht gestützten Antrag auf Berichtigung der Pseudonymisierung einer im RIS veröffentlichten OGH-Entscheidung zu stellen.

Beschluss vom 24.8.2022, 7 Ob 121/22b

In diesem Verfahren betreffend das Recht auf Erlassung einer einstweiligen Verfügung (die betroffene Person soll gegen die Antragstellerin gewalttätig geworden sein, was gegen ihren Willen durch Bilder einer Handykamera dokumentiert wurde) hatte sich der OGH mit der Frage zu befassen, ob die DSGVO ein Verbot beinhaltet, rechtswidrig erlangte (Bild-) Daten als Beweismittel zu verwerten.

Das Erstgericht hatte dies bejaht und den Antrag abgewiesen, weil weder die Standbilder noch der USB-Stick mit einer Videoaufzeichnung bewertet werden könnten, weil der Antragsgegner als gefilmte Person in die Verarbeitung der personenbezogenen Daten nicht aktiv eingewilligt habe.

Der OGH bestätigte nach einem ordentlichen Revisionsrekurs der betroffenen Person (Antragsgegner) die anderslautende und die Sache an das Erstgericht zurückverweisende Entscheidung des Rekursgerichts.

Nach ausführlicher Darlegung vorliegender Lehrmeinungen, die die Frage verneinen und dabei insbesondere Art. 9 Abs. 2 lit. f DSGVO für einen Größenschluss heranziehen, kam der OGH zu folgender Schlussfolgerung:

„Der erkennende Senat geht vor diesem Hintergrund davon aus, dass auch nach Inkrafttreten der DSGVO kein generelles Beweisverwertungsverbot für nach den Datenschutzbestimmungen rechtswidrig erlangte Beweismittel besteht. Die Klärung der Frage der Notwendigkeit einer Interessenabwägung vor dem Hintergrund des Inkrafttretens der DSGVO in einem Provisorialverfahren zum Schutz vor Gewalt kann dahingestellt bleiben, weil eine solche hier jedenfalls zugunsten der Antragstellerin ausginge.“

Urteil vom 29.08.2022, 6 Ob 198/21t

In dieser Entscheidung, die ebenfalls eine öffentlich zugängliche Datenverarbeitung für Zwecke der Bewertung betrifft, hat das Höchstgericht der Revision einer Betroffenen (Ärztin) und der Ärztekammer für Wien nicht Folge gegeben. Die Sache betrifft die Datenverarbeitung durch die Betreiberin (Ges.m.b.H.) eines Such- und Bewertungsportals für Ärzte (siehe auch DSB, 23.01.2019, DSB-D123.342/0001-DSB/2019, RIS). Der OGH hat eine umfassende Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO vorgenommen. Die Verantwortliche nimmt sowohl eigene berechtigte Interessen als auch solche der Nutzer ihres Portals wahr. Sie kann sich dabei sowohl auf Art. 11 GRC (Informationsfreiheit) als auch auf Art. 16 GRC (Unternehmerfreiheit) stützen. Die Verarbeitung ist notwendig, da es für den angestrebten Zweck auf eine möglichst vollständige Erfassung aller niedergelassenen Ärzte ankommt. Berechtigte Interessen der (Erst-) Klägerin und Betroffenen können sich auf Art. 7 und 8 GRC (Privatleben, Datenschutz) sowie ebenfalls Art. 16 GRC stützen. Diese überwiegen jedoch nicht. Die Verarbeitung betrifft nur die Sozialsphäre, nicht den höchstpersönlichen Lebensbereich der Ärztin. Ausschlaggebend war wohl das laut OGH „ganz erhebliche Interesse, das die Öffentlichkeit an den im Portal angebotenen Informationen und Möglichkeiten hat“, in Verbindung mit der Tatsache, dass die Verantwortliche ein Melde- und Beschwerdesystem zum Schutz gegen Missbrauch des Bewertungssystems eingerichtet hat.

Beschluss vom 5.12.2022, 5 Ob 178/22w

Dieser Beschluss des Höchstgerichts ist in einem Verfahren ergangen, in dem zwei Journalisten (der Revisionsrekurs an den OGH wurde nur von einem der beiden erhoben) gemäß § 5 Abs. 4 GUG bei einem Bezirksgericht Auskunft aus dem Personenverzeichnis des elektronischen Grundbuchs verlangt hatten.

Das Personenverzeichnis enthält die Daten aller Personen, die in Österreich Rechte an Liegenschaften (wie Alleineigentum, Miteigentum oder Wohnungseigentum) besitzen. Es ist, anders als das nach (Katastral-) Gemeinden und Liegenschaften geordnete Grundbuch selbst, nicht öffentlich einsehbar.

Die Antragsteller wollten wissen, ob 20 nach Namen und Geburtsdatum identifizierte Personen im Personenverzeichnis aufscheinen. Es handelte sich um als vermögend bekannte Personen, die zum Teil auf Sanktionslisten der EU (Anhang I zur Verordnung (EU) Nr. 269/2014) und von Drittstaaten wegen Unterstützung Russlands im Krieg gegen die Ukraine aufscheinen. Bei weiteren war angegeben, dass Verbindungen zu österreichischen Unternehmen und/oder Immobilien in Österreich bestehen würden. Als begründetes Interesse an der Auskunft wurde angegeben, dass überprüft werden sollte, ob diese Personen in Österreich Vermögen besitzen, und ob die entsprechenden Sanktionen von den österreichischen Behörden durchgesetzt werden. Es bestehet daher eine journalistische und ein öffentliches Informationsinteresse an diesen Daten.

Das Bezirksgericht und das Rekursgericht (Landesgericht für Zivilrechtssachen Wien) wiesen den Antrag ab, da kein rechtliches Interesse im Sinne der bisherigen Rechtsprechung (wie die Suche nach einem Vermögenswert, der im Zuge einer Vollstreckung gepfändet werden könnte) nachgewiesen worden sei.

Der OGH hat dem Revisionsrekurs hinsichtlich der Daten jener sechs Personen Folge gegeben, gegen die Sanktionen der EU gelten (Pflicht Österreichs zum Einfrieren von Vermögenswerten). Nach sorgfältigen Erwägungen und einer Interessenabwägung unter Zugrundelegung der Rechtsprechung des EGMR kommt das Höchstgericht zu dem Schluss, dass die durch Art. 10 Abs. 1 EMRK verfassungsrechtlich garantierte Informationsfreiheit im Hinblick auf die anerkannte Rolle der Medien als „public watchdog“ das (datenschutzrechtliche) Geheimhaltungsinteresse der betroffenen Personen soweit überwiegt, als überprüft werden soll, ob Österreich die von der EU verhängten Sanktionen auch durchsetzt (öffentliches Informationsinteresse).

Der OGH hat weiters verfahrensrechtlich entschieden, dass vor einer solchen Auskunft bzw. Einsichtgewährung die betroffene Person nicht gehört und in das Verfahren einbezogen werden muss. Keine Aussage hat der OGH zur Frage getroffen, ob die betroffene Person nach einer Auskunftserteilung gemäß Art. 13 f DSGVO u.a. über den Empfänger der Daten informiert werden muss.

Zur Frage einer weiterführenden Suche im Register wirtschaftlicher Eigentümer, siehe auch unten EuGH 22.11.2022, C-37/20 ua.

4.3 Verwaltungsgerichtshof

Der VwGH hat im Berichtsjahr entschieden, dass der DSB in amtswegig eingeleiteten Prüfverfahren nach österreichischem Verfahrensrecht keine Befugnis zukommt, über mögliche Abhilfe- oder Strafbefugnisse hinaus bereits beendete Rechtsverletzungen bescheidmäig festzustellen (und damit eine Klärung von Rechtsfragen zu ermöglichen). Nach Ansicht der DSB zeigt er damit eine Lücke im österreichischen Verfahrensrecht auf.

Im Verfahrenskomplex betreffend Beschwerden gegen die Verarbeitung von Daten zur statistisch errechneten „Parteiaffinität“ von tausenden Österreicherinnen und Österreichern durch ein großes Direktmarketingunternehmen dürfte der VwGH nun endgültig rechtliche Klarheit geschaffen haben (DSB für Beschwerdeverfahren wegen Verletzung des Rechts auf Geheimhaltung durch unrechtmäßige Datenverarbeitung auch nach Löschung entsprechender Daten zuständig, Feststellungsbescheide in diesem Fall zulässig).

Verfahren zur Frage der Auskunft betreffend automatisierte Entscheidungen und zu den Voraussetzungen der Bestrafung juristischer Personen (Erforderlichkeit des Nachweises des schuldhafoten Handelns einer verantwortlichen natürlichen Person) sind bis zum Abschluss von Vorabentscheidungsverfahren beim EuGH ausgesetzt worden.

Erkenntnis vom 8.2.2022, Ro 2021/04/0033

Die DSB hatte 2019 ein amtswegiges Prüfverfahren beim Betreiber eines Kundenbindungsprogramms („J*Club“) durchgeführt, und bescheidmäig Feststellungen betreffend die Berechtigung des Prüfverfahrens und die Rechtswidrigkeit bestimmter Datenverarbeitungen getroffen und dem Verantwortlichen aufgetragen, bestimmte Änderungen vorzunehmen, unter anderem das Profiling von Betroffenen, deren gültige Einwilligung nicht vorliegt, zu unterlassen. Der Bescheid wurde nach Einbringung einer Bescheidbeschwerde ohne grundlegende Änderungen durch eine genauer und enger gefasste Beschwerdevorentscheidung ersetzt. Insbesondere führte die DSB aus, es sei dem Betreiber nicht gestattet, eine Datenverarbeitung, die sich ausschließlich auf die Einwilligung der Betroffenen (Art. 4 Z 11 und Art. 6 Abs. 1 lit. a DSGVO) als Rechtsgrundlage stütze, bei Ungültigkeit oder Nichtvorliegen der Einwilligung nachträglich auf andere Gründe zu stützen. Eine Prüfung, ob solche nachträglich vorgebrachten Gründe vorliegen würden, sei daher nicht geboten.

Nach Vorlageantrag des Verantwortlichen gab das BVwG mit Erkenntnis vom 31.8.2021, Zl. W256 2227693-1 der Beschwerde statt und hob die Beschwerdevorentscheidung insgesamt ersatzlos auf. Die Revision wurde für zulässig erklärt. Nach der Rechtsansicht des BVwG hatte die DSB den Gegenstand des Prüfverfahrens zu eng gesehen und hätte auch prüfen müssen, ob andere Rechtfertigungsgründe gemäß Art. 6 Abs. 1 DSG vorliegen würden.

Gegen diese Entscheidung hat die DSB eine Amtsrevision eingebracht. Diese war teilweise erfolgreich. Der VwGH hat die Aufhebung der Beschwerdevorentscheidung hinsichtlich jener Spruchpunkte, die nicht rein feststellenden Charakter hatten, seinerseits aufgehoben.

Die Aufhebung der rein feststellenden Spruchpunkte sei rechtlich geboten gewesen, da die Ausübung der Abhilfebefugnis gemäß Art. 58 Abs. 2 lit. d DSGVO weder einen separaten Abspruch über die Berechtigung des amtswegigen Prüfverfahrens noch einen selbstständigen Abspruch über eine Feststellung betreffend das Nichtvorliegen eines bestimmten Erlaubnistaatbestandes des Art. 6 DSGVO bzw. die Unrechtmäßigkeit der Datenverarbeitung voraussetzt. Die Feststellung des Verstoßes bildet nur jeweils den Anlass für die Abhilfeentscheidung.

„Sache“ des Beschwerdeverfahrens vor dem BVwG war die Überprüfung der Rechtmäßigkeit der Ausübung der durch Art. 58 Abs. 2 lit. f DSGVO eingeräumten Abhilfebefugnis und damit verbunden die Frage, ob die betreffende Datenverarbeitung durch die Mitbeteiligte rechtmäßig im Sinne des Art. 6 DSGVO erfolgte. Das BVwG wäre daher berechtigt und verpflichtet gewesen, die entsprechende Prüfung selbst vorzunehmen und über die Rechtmäßigkeit der Datenverarbeitung zu entscheiden, statt den Bescheid ersatzlos zu beheben.

Beschluss vom 24.2.2022, Ra 2020/04/0187

In der Frage der Auslegung von Art. 83 DSGVO betreffend die Erforderlichkeit des Nachweises des schuldhaften Handelns einer konkreten Person zur Bestrafung eines Verbandes (Unternehmens), hat sich der VwGH eigentlich bereits im Sinne einer Bejahung der Frage festgelegt (Erkenntnis vom 12.5.2020, Ro 2019/04/0229).

Da beim EuGH inzwischen ein einschlägiges Vorabentscheidungsverfahren anhängig ist (Rechtssache C-807/21), hat der VwGH ein von der DSB anhängig gemachtes Revisionsverfahren bis zur Entscheidung des EuGH ausgesetzt.

Beschluss vom 3.3.2022, Ra 2020/02/0241

In dieser Entscheidung, die in einer straßenpolizeilichen Verwaltungsstrafsache ergangen ist, hat der VwGH ausdrücklich festgehalten, dass ausreichende einfachgesetzliche Grundlagen für die Datenverarbeitung durch die Verwaltungsstrafbehörden und das Verwaltungsgericht bestehen (einschließlich der Speicherung von Daten zu einschlägigen Vorstrafen). Diese Rechtsansicht wäre auch von der DSB in einem datenschutzrechtlichen Beschwerdeverfahren zu berücksichtigen.

Rechtssatz 4 des VwGH (RIS):

„Für Bezirksverwaltungsbehörden gibt es aufgrund einer Reihe von einfachgesetzlichen Bestimmungen (§ 26 Abs. 1 VStG, § 19 VStG, § 55 VStG) eine Rechtsgrundlage für die Datenverarbeitung im Zuge der Führung der Verwaltungsstrafverfahren in ihrem Zuständigkeitsbereich. § 26 VStG sieht die Zuständigkeit der Bezirksverwaltungsbehörden für die Führung von Verwaltungsstrafverfahren vor. Dabei haben diese gemäß § 19 VStG die Strafbemessung unter Berücksichtigung der in Betracht kommenden Erschwerungs- und Milderungsgründe und unter sinngemäßer Anwendung der §§ 32 bis 35 StGB vorzunehmen; demnach sind sie gesetzlich verpflichtet, Daten zu einschlägigen Vorstrafen zu berücksichtigen. Aus § 55 VStG ergibt sich zur Wahrnehmung der darin determinierten Aufgabe (Tilgung und ihrer Rechtsfolgen, insbesondere Nichtberücksichtigung einer getilgten Verwaltungsstrafe bei der Strafbemessung) die Verpflichtung zu einer ordnungsgemäßen Aufzeichnung der Daten der Verwaltungsstrafverfahren. Die Verarbeitung der Daten ist demnach für die Wahrnehmung der sich aus den Erfordernissen des Verwaltungsstrafverfahrens ergebenden Aufgabe, die im öffentlichen Interesse liegt, erforderlich (Art. 6 Abs. 1 lit. e iVm Abs. 3 DSGVO). Dass die Straßenverkehrssicherheit eine iSd. Art. 6 Abs. 1 lit. e DSGVO im öffentlichen Interesse liegende Aufgabe ist, hat auch der EuGH in einem Urteil vom 22. Juni 2021 bestätigt (vgl. EuGH 22.6.2021, Latvijas Republikas Saeima, C-439/19; VwGH 7.9.2021, Ra 2020/11/0213). Von einem unrechtmäßigen Eingriff in das Recht auf Geheimhaltung personenbezogener Daten durch die im Wege der Aktenführung erfolgte Datenverarbeitung im Zuge der Führung der Verwaltungsstrafverfahren im eigenen Zuständigkeitsbereich kann somit nicht die Rede sein. Das VwG verstößt durch die Verwertung der von einer BH übermittelten Daten zu einer einschlägigen Übertretung bei der Vornahme der Strafbemessung nicht gegen das Recht auf Geheimhaltung personenbezogener Daten nach dem DSG, weil das VwG zur Berücksichtigung einschlägiger

Verwaltungsvorstrafen zur Ermittlung der Strafzumessungsgründe im Rahmen des von ihm zu führenden Beschwerdeverfahrens gehalten ist.“

Beschluss vom 7.4.2022, Ro 2020/04/0010

In dieser Revisionssache, die den Umfang des Anspruchs auf Auskunft betreffend eine automatisierte Entscheidungsfindung durch eine Wirtschaftsauskunftei betrifft (insbesondere auch die Frage, ob und wie weit eine Auskunft über die involvierte Logik der Entscheidungsfindung im Hinblick auf Betriebs- und Geschäftsgeheimnisse verweigert werden darf), hat der VwGH das Verfahren bis zur Vorabentscheidung durch den Gerichtshof der Europäischen Union in den beiden Rechtssachen a) C-203/22 über das Ersuchen des Verwaltungsgerichts Wien vom 11. Februar 2022, VWG-101/042/791/2020-44, sowie b) in der Rechtssache C-634/21 über das Ersuchen des Verwaltungsgerichts Wiesbaden vom 1. Oktober 2021, 6 K 788/20.WI, ausgesetzt.

Erkenntnis vom 23.6.2022, Ro 2019/04/0221 und 0222

Ausgangspunkt dieser höchstgerichtlichen Entscheidung war ein amtsweiges Prüfverfahren der DSB, Verfahrenszahl DSB-D213.600, Bescheid vom 1.6.2018, GZ: DSB-D213.600/0001-DSB/2018. Darin war hinsichtlich der Nachfolge eines Arztes als für die Verarbeitung der Daten seiner Patienten Verantwortlicher festgestellt worden, dass ein in den Ruhestand tretender niedergelassener Arzt (1. Arzt) nicht berechtigt war, die Daten seiner Patientenkarteien (ärztliche Dokumentation gemäß § 51 ÄrzteG 1998) an eine Ärztin (2. Ärztin) zu übermitteln, die weder Kassenplanstellennachfolgerin noch Ordinationsstättennachfolgerin war, sondern lediglich im selben Wiener Bezirk eine neue Ordination eröffnet hatte. Die DSB hatte der 2. Ärztin aufgetragen, die Daten an den 1. Arzt zurückzustellen und danach zu löschen, sowie dem 1. Arzt aufgetragen, die Daten an seine Kassenplanstellennachfolgerin (mit neuer Ordinationsstätte) zu übermitteln.

Die Bescheidbeschwerde des 1. Arztes und der 2. Ärztin an das BVwG war soweit erfolgreich, als der Auftrag an den 1. Arzt (Übermittlung an Kassenplanstellennachfolgerin) mangels Rechtsgrundlage behoben und der Spruch neu gefasst wurde (Erkenntnis vom 3.4.2019, Zl. W258 2201288-1). Die ordentliche Revision wurde zugelassen und von beiden Ärzten auch ausgeführt (zuvor wurde eine Beschwerde an den VfGH mit dg. Beschluss vom 11.6.2019, E 1807/2019, abgelehnt).

Die Revision war jedoch nur insoweit erfolgreich, als der VwGH das angefochtene Erkenntnis im Umfang der bloßen Feststellung einer Rechtsverletzung unter Verweis auf seine Vorjukatur (Erkenntnis vom 14.12.2021, Ro 2020/04/0032) aufgehoben hat. Hinsichtlich des Leistungsauftrags (Rückabwicklung der Datenübermittlung) ist das Erkenntnis des BVwG bestätigt worden.

Dem Argument der Ärzte, die 2. Ärztin sei die „faktische Ordinationsstättennachfolgerin“ und daher gemäß § 51 Abs. 4 ÄrzteG 1998 zur Übernahme der Patientendaten legitimiert, hielt der VwGH Folgendes entgegen:

„Der angestrebte Zweck der Regelung, der nicht nur die Aufbewahrung der Patientendaten umfasst, sondern auch sicherstellen soll, dass die betroffenen Patienten im Falle des Bedarfs der Daten - etwa für eine Weiterbehandlung - in der Lage sind, den Aufbewahrungs-ort ohne langwierige Recherchen auch aufzufinden, schließt eine Interpretation dieser Wortwahl im Sinne der Revisionsausführungen aus. Der Sicherstellung der Verfügbarkeit der für eine spätere Behandlung der betroffenen Patienten allenfalls notwendigen Daten ist es nämlich gerade nicht dienlich, das Schicksal derselben von einem voluntativen Ele-

ment abhängig zu machen, dem etwa - wie es die Revision anspricht - eine „ökonomisch motivierte Unternehmensablöse“ zugrunde liegt. Der sicherzustellenden Auffindbarkeit durch den betroffenen Patienten ist nämlich nur dann gedient, wenn der Kreis der die Daten aufbewahrenden Personen von vornherein eindeutig festgelegt ist, was das Gesetz durch die Bezeichnung des Kassenplanstellennachfolgers und - subsidiär - des Ordinationsstätteninhabers gewährleisten will. [...]

Insofern die Revision ferner ausführt, der Gesetzgeber habe es unterlassen, an andere denkbare ärztliche Nachfolger zu denken und diese zur Übernahme der ärztlichen Dokumentation zu ermächtigen, und dass es angesichts der dramatischen Zunahme insbesondere von Wahlärzten geboten sei, diese offensichtlich planwidrige Lücke durch Analogie zu schließen, ist ihr wiederum entgegenzuhalten, dass § 51 Abs. 4 ÄrzteG 1998 nicht die Frage der Auswahl der Weiterbehandlung des Patienten betrifft, sondern die Sicherstellung der gesammelten Gesundheitsdaten bezweckt.“

Festzuhalten ist daher, dass die Patientendaten eines niedergelassenen Arztes (ohne Einwilligung der Patienten) nur an den Kassenplanstellennachfolger, sofern ein solcher nicht gegeben ist an den Ordinationsstättennachfolger übergeben werden dürfen. Eine freie wirtschaftliche Verwertung durch eine „ökonomisch motivierte Unternehmensablöse“ ist nicht zulässig.

Erkenntnis vom 23.6.2022, Ro 2022/04/0008

In dieser Sache hatte die betroffene Person, ein früherer Lehrer, beim Bundesministerium für Bildung, Wissenschaft und Forschung eine Dienstaufsichtsbeschwerde gegen eine Bildungsdirektion und eine Reihe dort tätiger Beamter wegen Mobbings erhoben. Zum Beweis seiner Vorwürfe legte der Betroffene u.a. Unterlagen zu seinem Gesundheitszustand vor. Die Bildungsdirektion (Revisionswerberin) übermittelte Kopien dieser Unterlagen (in Papierform) zwecks Vorbereitung einer Besprechung des weiteren Vorgehens an die anderen belangten Personen. Dagegen erhob der Betroffene Datenschutzbeschwerde wegen eines Eingriffs in sein Recht auf Geheimhaltung.

Die DSB wies diese Beschwerde unter Hinweis auf die Rechtsprechung zum sogenannten Übermaßverbot als unbegründet ab.

Das BVwG gab der dagegen erhobenen Bescheidbeschwerde des Betroffenen Folge, stellte „*eine unrechtmäßige Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie eine Verletzung des Grundrechts auf Datenschutz nach § 1 DSG*“ fest und trug der Revisionswerberin insbesondere auf, die Rückgabe und Vernichtung der betreffenden Unterlagen zu veranlassen (Erkenntnis vom 28.5.2020, Zl. W211 2216385-1).

Der VwGH änderte in tlw. Folgegebung der Revision der Bildungsdirektion den Spruch des BVwG dahingehend, dass er die Feststellung auf eine Verletzung des Rechts nach § 1 DSG einschränkte und den Leistungsauftrag zur Gänze behob.

Zur Begründung führte der VwGH aus, die getroffenen Feststellungen würden nicht für die Schlussfolgerung ausreichen, dass es sich bei der Übermittlung der Unterlagen zumindest um eine Datenverarbeitung in einem Dateisystem im Sinn von Art. 2 Z 1 und Art. 4 Z 6 DSGVO gehandelt hat. Da somit eine Überprüfung der Anwendbarkeit der DSGVO auf Basis des angefochtenen Erkenntnisses nicht möglich war, konnte der auf Art. 58 Abs. 2 DSGVO gestützte Leistungsauftrag keinen Bestand haben.

Die Feststellungen betreffend eine unrechtmäßige Verarbeitung besonderer Kategorien personenbezogener Daten waren hingegen nicht zulässig, da sie über den Antrag des

Betroffenen in der Bescheidbeschwerde, der lediglich eine Feststellung der Verletzung seines Geheimhaltungsrechts gemäß § 1 Abs. 1 DSG beantragt hatte, hinausgingen. Für einen Eingriff in letzteres Recht ist eine Datenverarbeitung in einem Dateisystem auch keine tatbestandsmäßige Voraussetzung. Mit Beschluss vom selben Tag, Ro 2020/04/0026, wurde die von der Datenschutzbehörde erhobene Amtsrevision gegen dasselbe Erkenntnis für gegenstandslos erklärt und das Verfahren eingestellt.

Beschluss vom 1.9.2022, Ra 2022/04/0066

Der VwGH hat hier eine Amtsrevision der DSB als unzulässig zurückgewiesen. Die DSB hatte in einem amtsweig eingeleiteten Prüfverfahren durch Bescheid die Rechtswidrigkeit einer von einer Aktiengesellschaft vorgenommenen Datenverarbeitung (Überwachung von Diensthandys und dienstlichen E-Mail-Accounts zwecks Ausforschung des Urhebers einer Indiskretion) festgestellt. Der entsprechende Vorgang lag in der Vergangenheit und war abgeschlossen, ein Auftrag zur Herstellung des rechtmäßigen Zustands gemäß Art. 58 Abs. 2 lit. d DSGVO (Abhilfebefugnis) kam nicht mehr in Betracht.

Das BVwG gab der Bescheidbeschwerde der Verantwortlichen Folge und hob den Bescheid der DSB unter Hinweis auf das Erkenntnis des VwGH vom 14.12.2021, Ro 2020/04/0032, auf (Erkenntnis vom 29.4.2022, Zl. W258 2247028-1).

Zur Unzulässigkeit der Revision gegen diese Entscheidung hielt der VwGH fest:

„Der von der Revision ins Treffen geführte Unterschied des dem Erkenntnis VwGH 14.12.2021, Ro 2020/04/0032 zugrundeliegenden Sachverhalts ändert somit nichts an der Anwendbarkeit des dort festgehaltenen Rechtssatzes auch im vorliegenden Fall. Insofern die Revision ausführt, es sei zu klären, ob es einer Aufsichtsbehörde im Rahmen eines amtsweigigen Prüfverfahrens möglich sei, „Sachverhalte zu prüfen und von einer Befugnis nach Art. 58 DSGVO Gebrauch zu machen, selbst wenn die Rechtsverletzung zum Zeitpunkt der Entscheidung bereits abgeschlossen ist und der Ausspruch einer Verwarnung nach Art. 58 Abs. 2 lit. b sowie die Verhängung einer Geldbuße nach Abs. 2 lit. i DSGVO nicht in Betracht kommen“, ist nicht ersichtlich, welche konkrete „Befugnis nach Art. 58 DSGVO“ die Revisionswerberin hier anspricht. Eine über den Katalog des Art. 58 DSGVO hinausgehende Befugnis wurde der Revisionswerberin als Aufsichtsbehörde im Sinne der DSGVO vom österreichischen Gesetzgeber nicht eingeräumt. Dass eine über die Ausführungen in Ro 2020/04/0032 hinausgehende Klarstellung der Rechtslage erforderlich wäre, wird hiermit nicht aufgezeigt.“

Erkenntnis vom 19.10.2022, Ro 2022/04/0001

In dieser Entscheidung aus dem Verfahrenskomplex der Verarbeitung von Daten zur „Parteiaffinität“ durch ein Direktmarketingunternehmen (Revisionswerberin) befasste sich der VwGH mit der Frage der – von der Revisionswerberin bestrittenen, von der DSB und vom BVwG (Erkenntnis vom 15.10.2021, Zl. W211 2233706-1) jedoch bejahten – Zuständigkeit der DSB für die Feststellung von in der Vergangenheit liegenden Verletzungen des Rechts auf Geheimhaltung (die Daten zur „Parteiaffinität“ waren nachweislich bereits vor der Entscheidung der DSB gelöscht worden).

Der VwGH hält dazu fest, dass § 24 Abs. 2 Z 5 DSG der betroffenen Person im Rahmen eines (Individual-) Beschwerdeverfahrens ausdrücklich ein Recht auf bescheidmäßige Feststellung einer Rechtsverletzung durch die DSB einräumt (anders im Fall eines amtsweigigen Prüfverfah-

rens, in dem der DSB laut Rechtsansicht des VwGH ein Feststellungsbescheid verwehrt ist, vgl. VwGH E 14.12.2021, Ro 2020/04/0032, und B 1.9.2022, Ra 2022/04/0066).

Bei den subjektiven Datenschutzrechten ist dabei zwischen solchen, die auf eine Leistung (insbesondere Auskunftserteilung, Löschung oder Berichtigung) abzielen – hier kann eine Klagstellung gemäß § 24 Abs. 6 DSG erfolgen – und dem Recht auf Geheimhaltung zu unterscheiden. Das Recht auf Geheimhaltung verkörpert kein Recht auf eine bestimmte Leistung, und die Geltendmachung einer Verletzung im Recht auf Geheimhaltung ist nicht auf eine Handlung des Verantwortlichen ausgerichtet. Eine erfolgte Verletzung durch unzulässige Ermittlung kann auch nicht durch eine Handlung (hier: Löschung der betreffenden Daten) gleichsam rückwirkend wieder beseitigt werden und unterscheidet sich damit von den datenschutzrechtlich gewährleisteten Rechten, denen durch eine bestimmte Leistung entsprochen werden kann.

Die DSB ist daher im Beschwerdeverfahren dafür zuständig, auch eine in der Vergangenheit liegende, bereits beendete Verletzung des Geheimhaltungsrechts zu untersuchen und die Rechtsverletzung durch Bescheid festzustellen. Die Revision wurde als unbegründet abgewiesen

4.4 Europäischer Gerichtshof für Menschenrechte

Im Berichtszeitraum hat der EGMR, soweit absehbar, keine für Aspekte des Datenschutzrechts bedeutende Entscheidung getroffen. Zur innerstaatlichen Umsetzung des bereits im Jahr 2021 ergangenen Urteil in der Sache Appl. 5434/17 (Volle Einsichtsmöglichkeit in den Inhalt eines Scheidungsfolgenvergleichs in der Urkundensammlung des Grundbuchs) siehe oben 4.2.

4.5 Europäischer Gerichtshof

Der EuGH hat im Berichtszeitraum insbesondere seine Rechtsprechung zum Geltungsbereich der DSGVO und zu den Möglichkeiten und Grenzen der grundrechtskonformen Gestaltung einer Vorratsdatenspeicherung für sicherheitspolizeiliche Zwecke vertieft. Er hat weiters eine wichtige Entscheidung zur Auslegung des Art. 55 Abs. 3 DSGVO in der Frage, was zur „justiziellen Tätigkeit“ der Gerichte zählt, getroffen. Es ergingen insgesamt 12 Urteile, wobei die wesentlichen in Folge dargestellt werden.

Urteil vom 24.2.2022, C-175/20

Ausgangsverfahren in dieser Sache war ein Streit zwischen einer Online-Plattform für private Kfz-Verkäufe und der lettischen Steuerbehörde, die den Betreiber verpflichtet hatte, Daten zu Anbietern von Kfz an sie zu übermitteln. Das lettische Verwaltungsgericht zweiter Instanz hatte dazu dem EuGH mehrere Auslegungsfragen vorgelegt.

Entscheidend sind in diesem Urteil wohl zwei Punkte: der EuGH hat erstens klargestellt, dass Ermittlungen einer Abgabenbehörde in den vollen Anwendungsbereich der DSGVO fallen, und eine solche Behörde dabei in Ermangelung einer ausdrücklichen Ermächtigung gemäß Art. 23 DSGVO im nationalen Recht nicht von der DSGVO, insbesondere nicht von den Grundsätzen des Art. 5 Abs. 1 DSGVO abweichen darf. Der EuGH hat zweitens betont, dass die Abgabenbehör-

de bei einer entsprechenden Anordnung insbesondere den Grundsatz der Datenminimierung (in Bezug auf die Dauer der Anordnung und den Umfang der zu übermittelnden Daten) einhalten und dies dem Übermittlungspflichtigen auch nachweisen muss (der EuGH spricht hier ausdrücklich in Rz 81 des Urteils von einer die Abgabenbehörde gemäß Art. 5 Abs. 2 DSGVO treffenden „*Beweislast*“).

Der Urteilstenor im Wortlaut:

1. *Die Bestimmungen 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) sind dahin auszulegen, dass die Erhebung von Informationen, die große Mengen personenbezogener Daten enthalten, durch die Steuerverwaltung eines Mitgliedstaats bei einem Wirtschaftsteilnehmer den Anforderungen dieser Verordnung, insbesondere deren Art. 5 Abs. 1, genügen muss.*
2. *Die Bestimmungen der Verordnung 2016/679 sind dahin auszulegen, dass die Steuerverwaltung eines Mitgliedstaats von Art. 5 Abs. 1 dieser Verordnung nicht abweichen darf, wenn ihr ein solches Recht nicht durch eine Gesetzgebungsmaßnahme im Sinne von Art. 23 Abs. 1 dieser Verordnung eingeräumt worden ist.*
3. *Die Bestimmungen der Verordnung 2016/679 sind dahin auszulegen, dass sie es der Steuerverwaltung eines Mitgliedstaats nicht verwehren, einen Anbieter eines Internet-Inseratdienstes zu verpflichten, ihr Informationen über die Steuerpflichtigen, die in einer der Rubriken seiner Website Inserate aufgegeben haben, offenzulegen, soweit insbesondere diese Daten für die spezifischen Zwecke, für die sie erhoben werden, notwendig sind und der Zeitraum, auf den sich die Datenerhebung bezieht, nicht länger ist, als dies zur Erreichung des angestrebten Ziels von allgemeinem Interesse unbedingt notwendig ist.*

Urteil vom 24.3.2022, C 245/20

Dieses Urteil betrifft die Auslegung von Art. 55 Abs. 3 DSGVO und die Reichweite des Begriffs „*justizielle Tätigkeit*“.

Anlassfall war eine Beschwerde von zwei betroffenen Personen bei der niederländischen Aufsichtsbehörde für Datenschutz (Autoriteit Persoonsgegevens - AP) gegen ein Gericht (Raad van State) wegen einer Medieninformation. Das Gericht hatte einem Journalisten auf dessen Anfrage die Beschwerdeführer betreffende, nicht-pseudonymisierte Unterlagen aus dem Akteninhalt eines laufenden Verfahrens übermittelt.

Die AP hatte sich unter Berufung auf Art. 55 Abs. 3 DSGVO für nicht zuständig erklärt. Außerdem hatte sie die Beschwerde an das aus ihrer Sicht zuständige richterliche Gremium beim Raad van State weitergeleitet. Das von den Beschwerdeführern gemäß Art. 78 Abs. 1 DSGVO angerufene Rechtsmittelgericht (Rechtbank Midden-Nederland) legte dem EuGH gemäß Art. 267 AEUV mehrere Fragen zur Vorabentscheidung vor.

Der EuGH legt Art. 55 Abs. 3 DSGVO hier vorrangig teleologisch aus, wobei Hauptgesichtspunkt die Sicherung der richterlichen Unabhängigkeit bei der Entscheidungsfindung ist: „*Zur Bestimmung der Tragweite des Begriffs der von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen im Sinne von Art. 55 Abs. 3 der Verordnung 2016/679 ist darauf hinzuweisen, dass bei der Auslegung einer Unionsrechtsvorschrift nicht nur ihr Wortlaut, sondern*

auch ihr Zusammenhang und die Ziele, die mit der Regelung, zu der sie gehört, verfolgt werden, zu berücksichtigen sind“ (Urteil, Rz 28 mwN).

„Folglich ist die Bezugnahme in Art. 55 Abs. 3 der Verordnung 2016/679 auf die von Gerichten „im Rahmen ihrer justiziellen Tätigkeit“ vorgenommenen Verarbeitungen im Kontext der Verordnung so zu verstehen, dass sie nicht auf die Verarbeitung personenbezogener Daten beschränkt ist, die von den Gerichten im Rahmen konkreter Rechtssachen durchgeführt wird, sondern in weiterem Sinn alle Verarbeitungsvorgänge erfasst, die von den Gerichten im Rahmen ihrer justiziellen Tätigkeiten vorgenommen werden, so dass Verarbeitungsvorgänge von der Zuständigkeit der Aufsichtsbehörde ausgeschlossen sind, deren Kontrolle durch diese Behörde mittelbar oder unmittelbar die Unabhängigkeit der Mitglieder oder der Entscheidungen der Gerichte beeinflussen könnte“ (Urteil, Rz 34, Unterstreichungen nicht im Original).

Der Urteilstenor im Wortlaut:

Art. 55 Abs. 3 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) ist dahin auszulegen, dass ein Gericht, das Journalisten vorübergehend Unterlagen aus einem Gerichtsverfahren bereitstellt, die personenbezogene Daten enthalten, um sie in die Lage zu versetzen, besser über den Ablauf des Gerichtsverfahrens zu berichten, seine „justizielle Tätigkeit“ im Sinne dieser Bestimmung ausübt.

Urteil vom 28.4.2022, C-319/20 (siehe auch Beschluss vom 31.05.2022, C-701/20)

In dieser Vorabentscheidungssache, vorgelegt vom deutschen Bundesgerichtshof, hat der EuGH entschieden, dass die DSGVO einer nationalen Regelung, nach der ein Verband zur Wahrung von Verbraucherinteressen gegen einen mutmaßlichen Datenschutzverletzer ohne entsprechenden Auftrag und unabhängig von der Verletzung konkreter Rechte betroffener Personen Klage mit der Begründung erheben kann, dass gegen das Verbot der Vornahme unlauterer Geschäftspraktiken, ein Verbraucherschutzgesetz oder das Verbot der Verwendung unwirksamer Allgemeiner Geschäftsbedingungen verstoßen worden sei, nicht entgegensteht, sofern die betreffende Datenverarbeitung die Rechte identifizierter oder identifizierbarer natürlicher Personen aus der DSGVO beeinträchtigen kann.

Das entsprechende nationale Gesetz muss demnach dem Verband nicht ausdrücklich eine objektive Klagsbefugnis zur Durchsetzung der DSGVO einräumen. Zwischenzeitig hat der Bundesgerichtshof den EuGH im selben Ausgangsrechtsstreit erneut angerufen (C-757/22).

Urteil vom 21.6.2022, C 817/19

Gegenstand dieser Sache waren Fragen der Grundrechtskonformität der Richtlinie (EU) 2016/681 (PNR-Richtlinie), die eine auf Fluggäste im internationalen Luftverkehr beschränkte Form der Vorratsdatenspeicherung vorsieht. Der belgische Verfassungsgerichtshof, bei dem eine Klage einer belgischen NGO gegen das belgische Durchführungsgesetz zur Umsetzung der PNR-Richtlinie anhängig war, hatte dem EuGH entsprechende Fragen zur Vorabentscheidung vorgelegt.

In seinem umfangreichen Urteil hält der EuGH fest, dass die Prüfung der vorgelegten Fragen nichts ergeben hat, was die Gültigkeit der PNR-Richtlinie an sich berühren könnte. Die in der PNR-Richtlinie vorgesehene Übermittlung, Verarbeitung und Speicherung von Daten kann auf das für die Bekämpfung terroristischer Straftaten und schwerer Kriminalität absolut Notwen-

dige beschränkt angesehen werden, sofern die in der Richtlinie vorgesehenen Befugnisse eng ausgelegt werden.

Die Verarbeitung darf nur für den Zweck der Prävention und Verfolgung terroristischer Straftaten und schwerer Kriminalität, wie in der PNR-Richtlinie umschrieben, erfolgen und nicht durch die nationale Gesetzgebung auf andere Formen der Kriminalität ausgedehnt werden. Dabei muss ein – zumindest mittelbarer – objektiver Zusammenhang mit der Beförderung von Fluggästen bestehen.

Nur im Fall des Bestehens einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung darf die Verarbeitung in einem begrenzten Zeitraum auf Flüge innerhalb der EU ausgedehnt werden.

Die Verarbeitung muss auf die in der PNR-Richtlinie angeführten, klar identifizierbaren und umschriebenen Informationen beschränkt bleiben.

Weiters hat der EuGH festgehalten, dass die nationale PNR-Zentralstelle bei der Vorabüberprüfung anhand im Voraus festgelegter Kriterien keine Technologien der künstlichen Intelligenz im Rahmen selbstlernender Systeme („machine learning“) heranziehen darf, die – ohne menschliche Einwirkung und Kontrolle – den Bewertungsprozess und insbesondere die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien ändern können.

Die PNR-Daten müssen regelmäßig, objektiv und diskriminierungsfrei überprüft werden und dürfen nur unter besonders strengen Kriterien nachträglich (nach einem Flug einer betroffenen Person) von den Sicherheitsbehörden angefordert werden.

Nur während eines Zeitraums von sechs Monaten überschreitet die Speicherung der PNR-Daten aller Fluggäste, für die das durch die PNR-Richtlinie geschaffene System gilt, grundsätzlich nicht die Grenzen des absolut Notwendigen. Eine längere Verarbeitung der PNR-Daten ist nur bei Vorliegen objektiver Anhaltspunkte (wie einem überprüften „Treffer“), die eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit einer Flugreise belegen können, zulässig. Eine generelle Speicherdauer von fünf Jahren erachtet der EuGH dagegen als grundrechtswidrig.

Schließlich führt der EuGH aus, dass das mit der PNR-Richtlinie geschaffene System nicht durch nationale Rechtsvorschriften generell auf andere Verkehrssysteme als den Luftverkehr ausgedehnt werden darf.

Urteil vom 22.6.2022, C-534/20

In dieser Sache hatte das deutsche Bundesarbeitsgericht den EuGH um die Auslegung von Art. 38 Abs. 3 Satz 2 DSGVO ersucht. Im Ausgangsverfahren war die Frage strittig, ob ein für den Datenschutzbeauftragten eines Unternehmens durch § 38 Abs. 1 und 2 in Verbindung mit § 6 Abs. 4 Satz 2 deutsches BDSG vorgesehener besonders strenger Kündigungsschutz mit dem Unionsrecht vereinbar ist. Art. 38 Abs. 3 Satz 2 DSGVO verbietet nur eine „Motivkündigung“ im Zusammenhang mit der Tätigkeit des Datenschutzbeauftragten. Eine solche lag im Anlassverfahren nicht vor.

Der EuGH hielt fest, dass es sich bei den relevanten nationalen Rechtsvorschriften um solche mit sozialpolitischen und nicht datenschutzpolitischen Zielen handelt. Auf diesem Rechtsgebiet komme dem nationalen Gesetzgeber ein Gestaltungsspielraum zu, solange er die Ziele

der DSGVO nicht vereitle, etwa die Abberufung eines ungeeigneten Datenschutzbeauftragten unmöglich mache.

Der Urteilstenor im Wortlaut:

Art. 38 Abs. 3 Satz 2 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) ist dahin auszulegen, dass er einer nationalen Regelung nicht entgegensteht, nach der einem bei einem Verantwortlichen oder einem Auftragsverarbeiter beschäftigten Datenschutzbeauftragten nur aus wichtigem Grund gekündigt werden kann, auch wenn die Kündigung nicht mit der Erfüllung seiner Aufgaben zusammenhängt, sofern diese Regelung die Verwirklichung der Ziele der DSGVO nicht beeinträchtigt.

Urteil vom 20.10.2022, C-306/21

Ausgangspunkt in diesem Rechtsstreit war die Frage, ob die DSGVO auf Sachverhalte im Zusammenhang mit der Durchführung nationaler Wahlen anzuwenden ist.

In Bulgarien hatten die nationale Datenschutzbehörde und die zentrale Wahlkommission eine Entscheidung erlassen, wonach die Massenmedien personenbezogene Daten durch Videoaufzeichnung nur bei Eröffnung des Wahltags, dessen Schließung, Feststellung der Ergebnisse der Stimmabgabe sowie der Höhe der laufenden Nummern der Stimmzettel verarbeiten dürfen. Allen anderen „Akteuren des Wahlverfahrens“ wurde eine Videoaufzeichnung jedoch untersagt, weil ihre Rolle im Wahlverfahren damit nicht vereinbar sei. Gegen diese Entscheidung hatte ein Bündnis politischer Parteien Klage erhoben; das oberste bulgarische Verwaltungsgericht legte dem EuGH mehrere Fragen zur Vorabentscheidung vor.

Zur Frage, ob die Verarbeitung personenbezogener Daten durch Videoaufzeichnung bei der Durchführung von Wahlen unter die in Art. 2 Abs. 2 lit. a DSGVO vorgesehene Ausnahme fällt, hat der EuGH seine Rechtsprechung, wonach diese Ausnahme eng auszulegen ist, erweitert. Art. 2 Abs. 2 lit a DSGVO ist in Verbindung mit Art. 2 Abs. 2 lit. b und Erwägungsgrund 16 zu lesen, wonach diese Verordnung nicht für die Verarbeitung personenbezogener Daten im Zusammenhang mit „Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, wie etwa die nationale Sicherheit betreffende Tätigkeiten, und den Tätigkeiten „im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der Union“ gilt. Auf praktisch alle anderen Sachverhalte (ausgenommen noch solche, die von der sogenannten „Haushaltsausnahme“ gemäß Art. 2 Abs. 2 lit. c DSGVO erfasst werden, sowie die Verarbeitung von Daten für Zwecke, die in der Datenschutzrichtlinie Polizei und Justiz, Richtlinie (EU) 2016/680, geregelt sind), ist die DSGVO demnach anwendbar.

Die Bestimmungen der DSGVO stehen weiters einer behördlichen Beschränkung von Videoaufzeichnungen bei einem Wahlakt nicht entgegen.

Der Urteilstenor im Wortlaut:

1. *Art. 2 Abs. 2 Buchst. a 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) ist dahin auszulegen, dass die Verarbeitung*

personenbezogener Daten im Zusammenhang mit der Durchführung von Wahlen in einem Mitgliedstaat nicht vom Anwendungsbereich dieser Verordnung ausgenommen ist.

2. *Art. 6 Abs. 1 Buchst. e und Art. 58 der Verordnung 2016/679 sind dahin auszulegen, dass diese Bestimmungen dem Erlass eines allgemeingültigen Verwaltungsakts durch die zuständigen Behörden eines Mitgliedstaats, der die Beschränkung oder gegebenenfalls das Verbot der Videoaufzeichnung der Stimmenauszählung in Wahllokalen bei Wahlen in diesem Mitgliedstaat vorsieht, nicht entgegenstehen.*

EuGH Urteil vom 22.11.2022, C-37/20, C-601/20

Auf Grundlage eines Vorabentscheidungsersuchens eines Luxemburger Gerichts hat der Gerichtshof in dieser Sache eine Bestimmung der novellierten Geldwäscherichtlinie für ungültig erklärt. Die für ungültig erklärte Bestimmung verpflichtete die Mitgliedstaaten, ein schon in einer früheren Fassung vorgesehenes Register wirtschaftlicher Eigentümer der Öffentlichkeit zugänglich zu machen. Die Entscheidung beruht auf zwei Klagen (des als wirtschaftlicher Eigentümer betroffenen WM und einer Gesellschaft) auf Sperre des öffentlichen Zugangs zu Daten des Registers wirtschaftlicher Eigentümer.

Zusammengefasst kommt der Gerichtshof zu dem Schluss, dass die Grundsätze der Beschränkung von Grundrechten (Gesetzmäßigkeit, Erforderlichkeit des Eingriffs, Bindung an bestimmte Zwecke, Verhältnismäßigkeit, Achtung des Wesensgehalts des Grundrechts) wie sie abgeleitet aus Art. 52 Abs. 1 GRC betreffend die Verarbeitung personenbezogener Daten in Art. 5 Abs. 1 DSGVO positiviert sind, zur Prüfung der Grundrechtskonformität (hier: im Hinblick auf Art. 7 und Art. 8 GRC) von Gesetzgebungsakten heranzuziehen sind. Hier hat der Gerichtshof stark mit Ziel und Zweck der geprüften Rechtsvorschrift (teleologisch) argumentiert, die nicht auf Transparenz (iSv Art. 1 und 10 EUV sowie Art. 15 AEUV), sondern auf Prävention (von Geldwäsche und Terrorismusfinanzierung) abzielt. Weder Rat noch Kommission hätten überzeugend darlegen können, inwiefern die unbeschränkte Öffentlichkeit eines Registers der wirtschaftlichen Eigentümer für diesen Präventionszweck erforderlich sei (sinngemäß: Verletzung der Grundsätze des Art. 5 Abs. 1 lit. b und c [Zweckbindung, Datenminimierung] der DSGVO). Der Betroffene WM habe demgegenüber zumindest darlegen können, dass die im Luxemburger Durchführungsgesetz vorgesehene Offenlegung seiner Daten als wirtschaftlicher Eigentümer einer Immobiliengesellschaft ihn und seine Familie einem unverhältnismäßigen Risiko von Betrug, Entführung, Erpressung, Schutzgelderpressung, Schikane, Gewalt oder Einschüchterung aussetze.

Informationen über die wirtschaftlichen Eigentümer müssen aber in jedem Fall (Mindestmaß) den zuständigen Behörden und den zentralen Meldestellen ohne Einschränkung sowie den Verpflichteten im Rahmen der Erfüllung der Sorgfaltspflichten gegenüber Kunden zwecks Verhinderung von Geldwäsche und Terrorismusfinanzierung zugänglich sein.

Als unmittelbares Ergebnis des Urteils hat in Österreich das Bundesministerium für Finanzen entschieden, § 10 WiEiReG, der auf der für ungültig erklärten Bestimmung beruht, nicht mehr anzuwenden und das österreichische Register der wirtschaftlichen Eigentümer für die öffentliche Einsichtnahme durch jedermann zu sperren.

Der Urteilstenor im Wortlaut:

- *Art. 1 Nr. 15 Buchst. c der Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinan-*

zierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU ist ungültig, soweit durch diese Bestimmung Art. 30 Abs. 5 Unterabs. 1 Buchst. c der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission dahin geändert wurde, dass dieser Art. 30 Abs. 5 Unterabs. 1 Buchst. c der Richtlinie 2015/849 in seiner so geänderten Fassung vorsieht, dass die Mitgliedstaaten sicherstellen, dass die Informationen über die wirtschaftlichen Eigentümer der in ihrem Gebiet eingetragenen Gesellschaften oder anderen juristischen Personen in allen Fällen für alle Mitglieder der Öffentlichkeit zugänglich sind.

5 Datenschutz-Grundverordnung und Datenschutzgesetz – Erfahrungen, legistische Maßnahmen, Projekte der Datenschutzbehörde

5.1 Allgemeine Erfahrungen der DSB im Berichtszeitraum, einschließlich Parlamentarischer Anfragen

Mit der weitgehenden Aufhebung der Einschränkungen im Zusammenhang mit Covid-19 konnte auch der Dienstbetrieb in der Datenschutzbehörde normalisiert werden.

Mit Oktober 2022 wurden alle behördlichen Restriktionen aufgehoben.

5.1.1 So genannte „Impf-Beschwerden“

Im Datenschutzbericht 2021 wurde darüber berichtet, dass die Datenschutzbehörde gegen Ende des Jahres 2021 zunächst mit rund 3.000, im Laufe des Jahres 2022 mit weiteren Beschwerden, sohin insgesamt 4.890 Beschwerden, befasst wurde, die alle auf die Zusendung personalisierter Schreiben, in welchen auf die Impfung gegen Covid-19 hingewiesen wurde, zurückzuführen waren.

Der Datenschutzbehörde gelang es durch eine gezielte Verfahrenskonzentration, diese Beschwerden im Laufe des Jahres 2022 weitgehend zu beenden (siehe dazu im Detail Kapitel 3.2.1.1).

Die Bearbeitung derartiger „Massenverfahren“ hat jedoch **verfahrensrechtliche Schwachstellen** offen gelegt. Die im Allgemeinen Verwaltungsverfahrensgesetz – AVG vorgesehenen Bestimmungen zur Verfahrenskonzentration (insbes. die Verbindung von Verfahren nach § 39 Abs. 2 AVG) sind für Verfahren in dieser Größenordnung unzureichend; die §§ 44a ff AVG, die „Großverfahren“ regeln, können auf das Beschwerdeverfahren nach Art. 77 DSGVO iVm § 24 DSG nicht angewendet werden, weil sie auf antragsgebundene Verfahren, bei welchen Einwendungen gemacht werden können (also idR Anlagengenehmigungsverfahren), abzielen, nicht jedoch auf kontradiktoriale Verfahren.

Eine Regelung wie in **§ 34 Abs. 3 VwGVG**, die eine gezielte Verfahrensführung ermöglicht, fehlt im AVG.

5.1.2. Strategische Befassung der Datenschutzbehörde

Im Jahr 2022 konnte in verstärktem Maße eine „**strategische Befassung**“ der Datenschutzbehörde festgestellt werden.

Darunter versteht die Datenschutzbehörde eine große Anzahl von Beschwerden nach Art. 77 DSGVO, die von einer Organisation im Sinne des Art. 80 Abs. 1 DSGVO eingebracht werden und sich zwar gegen unterschiedliche Beschwerdegegner richten, jedoch weitgehend denselben Beschwerdeinhalt aufweisen und deren Ziel darin besteht, die Beschwerdegegner und – aufgrund der mit der Verfahrensführung verbundenen Publizität (die Einleitung der Verfahren wird von der Organisation medial beworben) – auch andere zu einem rechtskonformen Verhalten anzuhalten.

Im Jahr 2022 betraf dies 116 Beschwerden gegen unterschiedliche Webseitenbetreiber, teilweise mit Sitz in Österreich, teilweise in anderen Mitgliedstaaten und teilweise in Drittstaaten, wegen mangelhafter Cookie-Banner.

Die Datenschutzbehörde ist verpflichtet, diese Beschwerden in Behandlung zu nehmen und einer Entscheidung zuzuführen. Da in jenen Fällen, in welchen der bezeichnete Beschwerdegegner seinen Sitz in einem anderen Mitgliedstaat hat, die Befassung der Aufsichtsbehörde vor Ort vorzunehmen ist, sind diese Verfahren mit einem hohen Koordinierungsaufwand verbunden.

Die hohe Anzahl der Verfahren, welche zusätzlich zu sonstigen Beschwerdeverfahren zu sehen ist, bedingte, dass hiefür eine eigene Arbeitsgruppe einzurichten war, um eine kohärente Verfahrensführung und Entscheidungsfindung zu gewährleisten.

Ein Teil dieser Verfahren konnte im Berichtszeitraum abgeschlossen werden.

5.1.3. Auswirkungen der Rechtsprechung des VwGH

Die vom VwGH mit Erkenntnis vom 14.12.2021, Ro 2020/04/0032, begründete und mit Beschluss vom 01.09.2022, Ra 2022/04/0066, bestätigte Judikaturlinie hat weitreichende Auswirkungen auf die Führung von amtswegigen Prüfverfahren durch die Datenschutzbehörde (siehe dazu auch Kapitel 4.3. des vorliegenden Berichts).

Nach dieser Rechtsprechung ist „Sache“ eines amtswegigen Prüfverfahrens nur, ob die Datenschutzbehörde von ihren Abhilfebefugnissen nach Art. 58 Abs. 2 DSGVO Gebrauch zu machen hat oder nicht. Es ist der Datenschutzbehörde jedoch verwehrt, im Rahmen eines solchen Prüfverfahrens eine Rechtsverletzung im Spruch lediglich festzustellen. Die in Art. 58 Abs. 2 DSGVO genannten Abhilfebefugnisse sind – bis auf drei Ausnahmen – auf zum Entscheidungszeitpunkt noch anhaltende Rechtsverletzungen ausgelegt.

Dies hat zur Folge, dass Verletzungen, die in der Vergangenheit liegen, jedoch zum Zeitpunkt der Entscheidung der Datenschutzbehörde nicht mehr andauern, in amtswegigen Prüfverfahren nicht mehr aufgegriffen werden können. Dies ist typischerweise bei Verletzungen im Recht auf Geheimhaltung bzw. bei Verstößen gegen Art. 5 und 6 DSGVO der Fall. In solchen Fällen ist demnach die Führung eines amtswegigen Verwaltungsverfahrens nicht möglich, solche Verletzungen können ausschließlich im Rahmen von Verwaltungsstrafverfahren geprüft werden. Aufgrund der Anordnung des § 30 Abs. 5 DSG ist dies jedoch bei Behörden und öffentlichen Stellen ausgeschlossen, sodass die beschriebenen Rechtsverletzungen bei diesen Verantwortlichen durch die Datenschutzbehörde amtswegig überhaupt nicht mehr aufgegriffen werden können.

Diese Lücke kann nur durch eine Novelle des DSG geschlossen werden.

5.1.4. Vorabentscheidungsersuchen an den EuGH

Das Jahr 2022 war, ebenso wie das Jahr 2021, gekennzeichnet von einem starken Anstieg der an den EuGH gerichteten Vorabentscheidungsverfahren zur Auslegung der DSGVO.

In 25 Fällen (2021: 27) richteten nationale (Höchst-)Gerichte Vorabentscheidungsersuchen an den EuGH. Darunter befinden sich auch drei Vorabentscheidungsersuchen aus Österreich:

- C-33/22, eingereicht vom Verwaltungsgerichtshof
- C-115/22, eingereicht von der Unabhängigen Schiedskommission Wien
- C-203/22, eingereicht vom Verwaltungsgericht Wien

Die Datenschutzbehörde ist Verfahrenspartei des Verfahrens zu C-33/22, in welchem es um zwei wesentliche Fragen geht:

- a) Ist die DSGVO auf die Datenverarbeitung durch (bestimmte) parlamentarische Untersuchungsausschüsse anwendbar?
- b) Kann die Datenschutzbehörde als zuständige Aufsichtsbehörde gegenüber parlamentarischen Untersuchungsausschüssen angesehen werden?

Diese Zahl belegt, dass nationale (Höchst-)Gerichte – ebenso wie im Jahr 2021 – in hohem Maße mit Auslegungsfragen zur DSGVO befasst sind und den EuGH ersuchen, dazu Stellung zu nehmen.

Das Jahr 2022 war aber auch gekennzeichnet von einer zunehmenden Anzahl an Urteilen (insgesamt: 12) des EuGH zur DSGVO, also im Schnitt ein Urteil pro Monat (siehe dazu im Detail Kapitel 4.5. des vorliegenden Berichts).

Beispielsweise seien folgende Entscheidungen erwähnt:

- Zur primärrechtlichen Konformität der Richtlinie (EU) 2016/681 (PNR-Richtlinie): Urteil vom 21.06.2022, C-817/19
- Zur Auslegung der Wortfolge „justizielle Tätigkeit“ in Art. 55 Abs. 3 DSGVO und damit einhergehend zur Unzuständigkeit der Aufsichtsbehörde: Urteil vom 24.03.2022, C-245/20
- Zur Klagebefugnis von Verbraucherschutzverbänden auf Grundlage der DSGVO: Urteil vom 28.04.2022, C-319/20
- Zur Kündigungs möglichkeit von Datenschutzbeauftragten: Urteil vom 22.06.2022, C-534/20
- Zur Anwendbarkeit der DSGVO auf nationale Wahlen: Urteil vom 20.10.2022, C-306/21

In folgenden, bereits im Datenschutzbericht 2021 erwähnten Verfahren, ergingen im Berichtszeitraum Schlussanträge:

- 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 sowie Möglichkeit einer Kartellbehörde, Verstöße gegen die DSGVO aufzugreifen: C-252/21
- Reichweite des (immateriellen) Schadenersatzes nach Art. 82 DSGVO: C-300/21

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

5.1.5. Beschwerden an die Volksanwaltschaft

In 12 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. In 7 Fällen wurde der Beschwerde Berechtigung zuerkannt.

5.1.6. Parlamentarische Anfragen

Im Jahr 2022 wurden folgende parlamentarische Anfragen an die Bundesministerin für Justiz gestellt, die (auch) die Tätigkeit der Datenschutzbehörde betrafen:

- 9636/J „Datenschutz und Persönlichkeitsrechte bei den Olympischen Winterspielen in China/Peking 2022“
- 10894/J „Klimaschutz ohne Datenschutz“
- 13102/J „Arbeitsanfall bei der DSB“

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 DSG 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.

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

5.2 EU-Projekt privacy4kids

Das EU-finanzierte Forschungsprojekt „privacy4kids - Rising awareness about privacy of children in the digital age“ wurde in Zusammenarbeit mit der Universität Wien, Institut für Innovation und Digitalisierung im Recht, und der österreichischen Datenschutzbehörde entwickelt. Die Projektergebnisse sind unter www.privacy4kids.at zu finden.

Projektgegenstand war zunächst die Erstellung und Veröffentlichung von animierten Lehrvideos zum Thema Privatsphäre und Datenschutz. Die Lehrvideos wurden jeweils für die Alterszielgruppe 6 bis 10 und 10 bis 14 Jahren erstellt und sollen auf unterhaltsame Art und Weise erklären, warum der Schutz personenbezogener Daten wichtig ist, welche Betroffenenrechte es gibt, welche Gefahren für die Privatsphäre im Internet bestehen und wie man sich zB. vor Betrug im Netz und Manipulation in sozialen Medien schützen kann.

Alle Videos wurden im Rahmen einer workshopartigen Lehrveranstaltung durch Studierende verschiedener Studienrichtungen erstellt. Lektor:innen und externe Expert:innen aus verschiedenen, relevanten Bereichen begleiteten diesen Prozess kontinuierlich.

Unter allen Videos finden sich weiterführende Informationen zum jeweiligen Thema. Darüber hinaus wurde ein Leitfaden für Lehrer:innen entwickelt, der diese dabei unterstützt, das

Thema im Unterricht zu behandeln. Konkret wird empfohlen, ein bis zwei Videos während des Unterrichts abzuspielen und im Anschluss eine kurze Diskussion zu führen. Im Leitfaden sind pro Video mehrere Beispiele angeführt, die im Rahmen der Diskussion angesprochen werden können. Während der „KinderUniWien2022“ haben Mitarbeitende der Universität Wien und der Datenschutzbehörde das Projekt in zwei Schulklassen erfolgreich vorgestellt.

Schließlich wurde das Projekt im Wintersemester 2022 erweitert. Im Zuge einer Lehrveranstaltung an der Universität Wien wurde ein (physisches) Datenschutz-Kartenspiel namens „PRIVO“ entwickelt, welches auf den Lehrvideos aufbaut. Auf jeder Spielkarte ist ein QR-Code vorhanden, der zu einem – zum Inhalt der Karte passenden – Lehrvideo samt weiteren Informationen führt.

Das Datenschutz-Kartenspiel wurde ebenfalls auf der Projektwebsite www.privacy4kids.at veröffentlicht. Darüber hinaus wurden einige Spielausgaben gedruckt und an ausgewählte Stakeholder und Schulen verschickt. **Vertreter von Schulen können physische Ausgaben anfragen, solange der Vorrat reicht. Weitere Informationen finden Sie auf der Projektwebsite.**

6 Europäische Zusammenarbeit

6.1 Europäische Union

6.1.1 Der Europäische Datenschutzausschuss

Der Europäische Datenschutzausschuss (EDSA) hat sich im Jahr 2022 15 Mal getroffen. Es fanden sechs Treffen vor Ort in Brüssel statt, die restlichen Plenarsitzungen wurden via Videokonferenz abgehalten.

Die im Rahmen dieser Treffen besprochenen Themen und angenommenen Dokumente wurden in den 11 Experten-Untergruppen des EDSA vorbereitet, die einander im Jahr 2022 rund 200 Mal überwiegend per Videokonferenz getroffen haben. Eine Auswahl dieser Dokumente wird im Folgenden näher genannt und dargelegt.

Zudem trafen sich die Mitglieder des EDSA im April 2022 in Wien, um Strategien für eine bessere Durchsetzung der DSGVO und eine noch engere grenzüberschreitende Zusammenarbeit zu besprechen. Dabei vereinbarten sie im Rahmen der Wiener Erklärung zur Zusammenarbeit bei der Durchsetzung (28. April 2022) eine verstärkte Zusammenarbeit bei strategischen Fällen, einen Ausbau der Kooperationsmethoden sowie eine bessere Abstimmung der nationalen Durchsetzungsstrategien. Darüber hinaus wurde beschlossen, eine Liste von Verfahrensaspekten zu erarbeiten, die im EU-Recht weiter harmonisiert werden könnten, um die Zusammenarbeit im Kooperationsmechanismus zu stärken. Diese Liste wurde der Europäischen Kommission im Oktober 2022 zur Prüfung vorgelegt, die Europäische Kommission nahm sie in das Arbeitsprogramm für 2023 auf.

Der EDSA hat im vergangenen Jahr 5 verbindliche Beschlüsse gemäß Artikel 65 Absatz 1 lit. a DSGVO³³ erlassen:

1. über den Entwurf eines Beschlusses der französischen Aufsichtsbehörde bezüglich Accor SA (1/2022, 15. Juni 2022): Die französische Aufsichtsbehörde hatte aufgrund einer bei der polnischen Aufsichtsbehörde eingebrachten Beschwerde über Schwierigkeiten bei der Ausübung der Rechte auf Widerspruch gegen Postwerbesendungen und Auskunft gegen Accor als federführende Behörde in diesem Verfahren einen Entscheidungsentwurf vorgelegt, gegen den die polnische Aufsichtsbehörde Einspruch betreffend die, ihrer Ansicht nach zu geringe Höhe der Geldbuße erhob. Der EDSA entschied unter anderem, dass die französische Aufsichtsbehörde die Elemente, auf die sie sich bei der Berechnung der Höhe der Geldbuße stützte, neu bewerten müsse, um die Erfüllung des Kriteriums der Abschreckung (Art. 83 DSGVO) sicherzustellen. Schließlich verhängte die französische Aufsichtsbehörde eine Geldbuße in Höhe von 500 000 Euro.
2. über den Entwurf eines Beschlusses der irischen Aufsichtsbehörde in Bezug auf Meta Platforms Ireland Limited (Instagram) (2/2022, 28. Juli 2022): Nach mehreren Einsprüchen betroffener Aufsichtsbehörden hielt der EDSA zum Entcheidungsentwurf

33 Siehe hierzu https://edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_en?f%5B0%5D=opinions_date%3A2022.

der irischen Aufsichtsbehörde fest, dass sich Meta Platforms Ireland Limited im Hinblick auf die Veröffentlichung von E-Mail-Adressen und/oder Telefonnummern von Kindern, die Instagram-Geschäftskonten betreiben, nicht auf Art. 6 Abs. 1 lit. b DSGVO (Erfüllung eines Vertrags) oder Art. 6 Absatz 1 lit. f DSGVO (berechtigte Interessen) stützen könne und stellte infolge der unrechtmäßigen Verarbeitung von personenbezogenen Daten von Kindern eine Verletzung des Art. 6 Abs. 1 DSGVO fest. Der EDSA forderte die irische Aufsichtsbehörde daher auf, die Festsetzung der Geldbuße in diesem Fall zu überprüfen. In ihrer endgültigen Entscheidung verhängte die irische Aufsichtsbehörde gegen Meta Platforms Ireland Limited eine Geldbuße in Höhe von 405 Millionen Euro.

3. über die von der irischen Aufsichtsbehörde vorgelegte Streitsache betreffend Meta Platforms Ireland Limited und ihres Facebook-Dienstes (3/2022, 5. Dezember 2022) und
4. über die von der irischen Aufsichtsbehörde vorgelegte Streitsache betreffend Meta Platforms Ireland Limited und ihres Instagram-Dienstes (4/2022, 5. Dezember 2022): Diese Entscheidungen des EDSA waren Untersuchungen der irischen Aufsichtsbehörde infolge zweier bei der österreichischen und belgischen Aufsichtsbehörde eingebrochener Beschwerden in Bezug auf die Rechtmäßigkeit und Transparenz der Datenverarbeitung zum Zwecke der personalisierten Werbung durch Meta Platforms Ireland Limited vorangegangen. Nachdem mehrere Aufsichtsbehörden Einsprüche gegen die beiden Entscheidungsentwürfe der irischen Aufsichtsbehörde erhoben hatten, entschied der EDSA, dass sich Meta Platforms Ireland Limited im Zusammenhang mit den Nutzungsbedingungen von Facebook und Instagram nicht auf einen Vertrag als Rechtsgrundlage für die Verarbeitung personenbezogener Daten zum Zweck personalisierter Werbung berufen könne, da dies kein Kernelement der Dienste sei. Folglich wurde festgehalten, dass Daten daher unrechtmäßig verarbeitet worden seien und die irische Aufsichtsbehörde aufgefordert, in beiden Fällen einen Verstoß gegen Art. 6 Abs. 1 DSGVO und den Grundsatz von Treu und Glauben gemäß Art. 5 Abs. 1 lit. a DSGVO festzustellen und Meta Platforms Ireland Limited anzuweisen, die Verarbeitung personenbezogener Daten für personalisierte Werbung im Rahmen der Dienste von Facebook und Instagram innerhalb von drei Monaten in Einklang mit den Bestimmungen der DSGVO zu bringen. Im Hinblick auf einen möglichen Verstoß gegen die Pflichten des Verantwortlichen bei der Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DSGVO wies der EDSA die irische Aufsichtsbehörde an, eine Untersuchung durchzuführen. Der EDSA stellte diesbezüglich fest, dass die schwerwiegenden Verstöße gegen die Transparenzverpflichtungen die berechtigten Erwartungen der Nutzer beeinträchtigt hätten, dass Meta Platforms Ireland Limited seine Dienste den Nutzern in irreführender Weise dargestellt habe und dass das Verhältnis zwischen Meta Platforms Ireland Limited und den Nutzern unausgewogen gewesen sei. In Bezug auf die Geldbußen wies der EDSA die irische Aufsichtsbehörde an, diese für die zusätzlichen Verstöße gegen Artikel 6 Abs. 1 DSGVO sowie gegen die Transparenzverpflichtungen zu verhängen, um den Erfordernissen der Wirksamkeit, Verhältnismäßigkeit und Abschreckung zu entsprechen. Die irische Aufsichtsbehörde verhängte gegen Meta Platforms Ireland Limited in ihrer endgültigen Entscheidung zu Facebook eine Geldbuße in Höhe von 210 Millionen Euro und in ihrer endgültigen Entscheidung zu Instagram einer Geldbuße in Höhe von 180 Millionen Euro.

5. über die von der irischen SA eingereichte Streitsache über WhatsApp Ireland Limited (5/2022, 5. Dezember 2022): Nachdem mehrere Aufsichtsbehörden Einsprüche betreffend einen Entscheidungsentwurf der irischen Aufsichtsbehörde im Zuge einer bei der deutschen Aufsichtsbehörde eingebrachten Beschwerde erhoben hatten, hielt der EDSA in seinem Beschluss zur Frage der Rechtmäßigkeit der Verarbeitung zu Zwecken der Serviceverbesserung fest, dass WhatsApp Ireland Limited sich unzulässigerweise auf einen Vertrag als Rechtsgrundlage für die Verarbeitung personenbezogener Daten gestützt habe. Infolgedessen wies der EDSA die irische Aufsichtsbehörde an, einen Verstoß gegen Art. 6 Abs. 1 DSGVO festzustellen und WhatsApp Ireland Limited anzuweisen, die Datenverarbeitung innerhalb einer Frist von drei Monaten in Einklang mit den Bestimmungen der DSGVO zu bringen. Zudem wurde die irische Aufsichtsbehörde aufgefordert, in ihre endgültige Entscheidung einen Verstoß gegen den Grundsatz der Fairness gemäß Art. 5 Abs. 1 lit. a DSGVO aufzunehmen und infolgedessen auch den Verstoß gegen die DSGVO mit einer Geldbuße zu ahnden. Der EDSA trug der irischen Aufsichtsbehörde ferner auf, eine Untersuchung im Hinblick auf die Verarbeitungen besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) sowie auf die Datenverarbeitung für Zwecke der personalisierten Werbung, für Marketingzwecke sowie für die Weitergabe von Statistiken an Dritte und den Austausch von Daten mit verbundenen Unternehmen zum Zwecke der Verbesserung von Dienstleistungen durch WhatsApp Ireland durchzuführen. In ihrer endgültigen Entscheidung stellte die irische Aufsichtsbehörde eine Verletzung des Art. 6 Abs. 1 DSGVO durch WhatsApp Ireland Limited fest und verhängte eine Geldbuße in Höhe von 5,5 Millionen Euro.

Des Weiteren hat der EDSA gemäß Art. 64 Abs. 1 DSGVO 2020 zu folgenden Themen insgesamt 31 *Stellungnahmen*³⁴ abgegeben:

- 3 Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Überwachung von Verhaltensregeln gemäß Art. 41 DSGVO (Bulgarien, Luxemburg, Slowenien);
- 2 Stellungnahmen zu nationalen Zertifizierungskriterien (Luxemburg, Deutschland);
- 3 Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Zertifizierung gemäß Art. 43 Abs. 1 lit. b DSGVO (Bulgarien, Frankreich und Polen);
- 23 Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (2 Mal WEB-HELP, Norican Group, Lundbeck Group, Groupon International Limited, MOL Group, 2 Mal Bioclinica Group, Fresenius Group, ANTOLIN Group, Daimler Truck Group, Mercedes-Benz Group, 2 Mal Ellucian Group, Hilti Group, 2 Mal Samres Group, Munich Re Reinsurance Group, LEYTON Group, DSV Group, 2 Mal Piano Group, Ramboll Group).

Gemäß Art. 64 Abs. 2 DSGVO 2020 hat der EDSA eine *Stellungnahme*³⁵ zur Genehmigung eines Europäischen Datenschutzsiegels gemäß Art. 42 Abs. 5 DSGVO (Europolprivacy) angenommen.

34 Siehe hierzu https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de?f%5B0%5D=opinions_date%3A2022&f%5B1%5D=opinions_publication_type%3A61

35 Siehe hierzu https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282022-europolprivacy-criteria-certification_de

Gemeinsam mit dem Europäischen Datenschutzbeauftragten (EDSB) hat der EDSA folgende *Stellungnahmen*³⁶ abgegeben:

- zur Verlängerung der Verordnung über das digitale COVID-Zertifikat der EU (1/2022, März 2022): Nach Ansicht des EDSA und des EDSB bewirke der Vorschlag keine wesentliche Änderung der Bestimmungen der Verordnung in Bezug auf die Verarbeitung personenbezogener Daten. Wie in der Stellungnahme betreffend die Verordnung zum ursprünglichen COVID-Zertifikat erinnern sie daran, dass die Einhaltung der Datenschutzvorschriften kein Hindernis für die Bekämpfung der COVID-19-Pandemie darstelle. Im Hinblick auf die Verlängerung der Maßnahme zur Bekämpfung der COVID-19-Pandemie sollten jedoch die einschlägigen wissenschaftlichen Erkenntnisse und die bestehenden zusätzlichen Maßnahmen regelmäßig bewertet werden, um die Einhaltung der allgemeinen Grundsätze der Wirksamkeit, Erforderlichkeit und Verhältnismäßigkeit zu gewährleisten. Weiters bedauern der EDSA und der EDSB, dass die Kommission keine Datenschutzfolgenabschätzung durchgeführt habe. Außerdem sprechen sie sich dafür aus, dass der alljährlich von der Europäischen Kommission an das Europäische Parlament und an den Rat vorzulegende Bericht über die Auswirkungen der Verordnung auf die Erleichterung der Freizügigkeit, die Wahrnehmung der Grundrechte und die Diskriminierungsfreiheit dem aktuellen Verordnungsvorschlag beigefügt werden sollte.
- zum Vorschlag des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für den fairen Zugang zu und die faire Nutzung von Daten (Data Act) (2/2022, 4. Mai 2022): Der EDSA und der EDSB fordern die Gesetzgeber auf, dafür zu sorgen, dass insbesondere bei der Verarbeitung von sensiblen personenbezogenen Daten die Rechte der betroffenen Personen geschützt werden. Darüber hinaus sollten die Produkte so gestaltet sein, dass den betroffenen Personen die Möglichkeit geboten werde, die Geräte anonym oder mit möglichst geringem Eingriff in die Privatsphäre zu nutzen. Der Zugang, die Verwendung und die gemeinsame Nutzung personenbezogener Daten durch andere Stellen sollte in voller Übereinstimmung mit allen Datenschutzgrundsätzen und -vorschriften erfolgen. Der EDSA und der EDSB raten den Gesetzgebern, Beschränkungen oder Einschränkungen für die Verwendung von Daten vorzusehen, die durch die Nutzung eines Produkts oder einer Dienstleistung durch andere Stellen als die betroffenen Personen generiert würden, insbesondere wenn die Daten genaue Rückschlüsse auf das Privatleben der betroffenen Personen zulassen oder anderweitig hohe Risiken für die Rechte und Freiheiten der betroffenen Personen mit sich bringen würden. Sie empfehlen daher die Einführung klarer Beschränkungen für die Verwendung der betreffenden Daten zu Zwecken des Direktmarketings, der Mitarbeiterüberwachung, der Berechnung und Änderung von Versicherungsprämien und der Prüfung der Kreditwürdigkeit. Beschränkungen der Datennutzung sollten auch zum Schutz besonders schutzbedürftiger Personen, insbesondere Minderjähriger, vorgesehen werden. Der EDSA und der EDSB äußern zudem große Bedenken hinsichtlich der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit der Verpflichtung, den öffentlichen Einrichtungen der EU-Mitgliedstaaten und den Organen, Einrichtungen, Ämtern und Agenturen der EU (EWR) im Falle eines „außergewöhnlichen Bedarfs“ Daten zur Verfügung zu stellen. In ihrer gemeinsamen Stellungnahme betonen sie, dass jede Einschränkung des Rechts auf den Schutz personenbezogener Daten eine Rechtsgrundlage erfordere, die angemessen zugänglich und vorhersehbar

³⁶ Siehe hierzu https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de?f%5B0%5D=opinions_date%3A2022&f%5B1%5D=opinions_publication_type%3A553

sein müsse. Die Rechtsgrundlage müsse auch den Umfang und die Art und Weise der Ausübung von Befugnissen durch die zuständigen Behörden festlegen und mit Garantien zum Schutz der betroffenen Personen vor willkürlichen Eingriffen einhergehen. Die Gesetzgeber werden nachdrücklich aufgefordert, die Voraussetzungen für einen Notfall oder einen „außergewöhnlichen Bedarf“ sowie die Frage, welche öffentlichen Stellen und EU-Institutionen in der Lage sein sollten, Daten anzufordern, sehr viel strenger zu definieren. Im Hinblick auf die Durchsetzung begrüßen der EDSA und der EDSB die Benennung von Datenschutzaufsichtsbehörden als zuständige Behörden, die für die Überwachung der Anwendung des Datenschutzgesetzes zuständig seien, soweit es den Schutz personenbezogener Daten betreffe. Die Mitgesetzgeber werden schließlich aufgefordert, die nationalen Datenschutzbehörden als koordinierende zuständige Behörden im Rahmen des Datenschutzgesetzes zu benennen.

- zum Vorschlag für eine Verordnung über den Europäischen Gesundheitsdatenraum (EHDS) (3/2022, 12. Juli 2022): Der EDSA und der EDSB begrüßen zunächst die Intention des Vorschlags, die Kontrolle des Einzelnen über seine personenbezogenen Gesundheitsdaten zu stärken. Allerdings halten sie in ihrer Stellungnahme auch fest, dass die in Kapitel IV des Vorschlags geschilderten Weiterverarbeitungstätigkeiten nicht ohne Risiken für die Rechte und Freiheiten natürlicher Personen seien, und, dass den ohnehin komplexen Bestimmungen über die Verarbeitung von Gesundheitsdaten nunmehr eine weitere Ebene derartiger Bestimmungen hinzugefügt wird. Daher betonen sie die Notwendigkeit, das Verhältnis zwischen den Bestimmungen des Vorschlags, jenen der DSGVO und dem innerstaatlichen Recht der Mitgliedstaaten sowie zu den laufenden europäischen Initiativen zu klären. Aufgrund der großen Menge an elektronischen Gesundheitsdaten, die verarbeitet würden sowie wegen ihrer hochsensiblen Natur, des Risikos unrechtmäßiger Datenzugriffe und der Notwendigkeit, eine wirksame Aufsicht durch unabhängige Datenschutzbehörden in vollem Umfang sicherzustellen, ersuchen der EDSA und der EDSB das Europäische Parlament und den Rat den Vorschlag dahingehend zu ergänzen, dass elektronische Gesundheitsdaten unbeschadet ihrer etwaigen Weiterübermittlung im Einklang mit Kapitel V DSGVO im EWR gespeichert werden müssen. Bezuglich der Zwecke der Sekundärnutzung von Gesundheitsdaten sind der EDSA und der EDSB der Ansicht, dass der Vorschlag keine angemessene Abgrenzung der Zwecke, zu denen elektronische Gesundheitsdaten weiterverarbeitet werden dürfen, enthalte. Die gesetzgebenden Organe sollten diese Zwecke daher näher eingrenzen und präzisieren. Schließlich müssten auch die Aufgaben und Zuständigkeiten der neuen öffentlichen Stellen sorgfältig angepasst werden, wobei insbesondere die Aufgaben und Zuständigkeiten der nationalen Aufsichtsbehörden, des EDSA und des EDSB bei der Verarbeitung von Gesundheitsdaten zu berücksichtigen seien. Dabei werde hervorgehoben, dass die Datenschutzbehörden die einzigen für Datenschutzfragen zuständigen Behörden seien und in derartigen Fragen auch die einzige Anlaufstelle für Einzelpersonen bleiben sollen.
- zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (4/2022, 28. Juli 2022): Der EDSA und der EDSB haben in ihrer Stellungnahme die Wichtigkeit des Themas betont, gleichzeitig aber auch Bedenken hinsichtlich der Notwendigkeit und Verhältnismäßigkeit der geplanten Maßnahmen und der Auswirkungen auf die Verschlüsselung von Online-Kommunikation geäußert. Empfohlen wurde zudem, dass der Vorschlag das Verhältnis zwischen den Aufgaben der Koordinierungsbehörden und denen der Datenschutzbehörden klären und dass die Übermittlung personenbezogener Daten zwischen der EU-Zentralstelle und Euro-

pol nur auf Einzelfallbasis erfolgen sollte.

Zudem hat der EDSA 2022 zu folgenden Themen *Leitlinien*³⁷ verabschiedet:

- zu den Rechten der Betroffenen: Recht auf Auskunft (1/2022, 28. Jänner 2022): Diese Leitlinie befasst sich mit drei Komponenten:
 - Mit der Bestätigung, ob Daten über die betreffende Person verarbeitet wurden oder nicht;
 - mit dem Zugang zu personenbezogenen Daten und
 - dem Zugang zu Informationen über deren Verarbeitung wie Zweck, Datenkategorien,
 - Empfänger und Dauer der Verarbeitung.

Die verschiedenen Abschnitte der Leitlinien sollen einen allgemeinen Überblick über das Recht auf Auskunft verschaffen sowie den Inhalt des Artikels selbst näher analysieren. Überdies analysieren die darauffolgenden Abschnitte die häufigsten Fragen und Problemstellungen im Zusammenhang mit der Umsetzung des Rechts auf Auskunft.

- zur Anwendung des Artikel 60 DSGVO (2/2022, 14. März): Diese Leitlinie 02/2022 unterstützt die wirksame Durchsetzung der effizienten Zusammenarbeit zwischen den nationalen Aufsichtsbehörden (SAs). Sie enthält eine ausführliche Beschreibung der Zusammenarbeit zwischen den Aufsichtsbehörden im Rahmen der Datenschutz-Grundverordnung und zielt darauf ab, die kohärente Anwendung der Rechtsvorschriften im Zusammenhang mit dem Mechanismus der einzigen Anlaufstelle für den Betroffenen und den Verantwortlichen weiter zu verbessern. Dadurch hilft sie den Aufsichtsbehörden, ihre eigenen nationalen Verfahren so auszulegen und anzuwenden, dass sie mit der Zusammenarbeit im Rahmen des Mechanismus der einzigen Anlaufstelle übereinstimmen.
- Betroffene und Verantwortliche zu Dark patterns in Benutzeroberflächen von Social-Media Plattformen: Wie man sie erkennt und vermeidet (3/2022, 14. März 2022, in öffentlicher Konsultation): Diese Leitlinie bietet praktische Empfehlungen zur Bewertung und Vermeidung sogenannter „deceptive design patterns“ auf Social-Media-Plattformen. Das umfassende Dokument stellt den Lebenszyklus eines Social Media Accounts (von der Anmeldung bis zur Abmeldung des Accounts) sowie der im Rahmen dieser zu beachtenden datenschutzrechtlicheren Prinzipien (Rechenschaftspflicht, Transparenz, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) dar. Die Leitlinie enthält zudem in ihrem Anhang eine Liste verschiedener Kategorien von „deceptive design patterns“ (Overloading, Skipping, Stirring, Hindering, Fickle, Left in the dark) und Best Practices.
- zur Berechnung von Geldbußen nach der DSGVO (4/2022, 12. Mai 2022): Diese Leitlinien sollen den „Ausgangsbetrag“ für die weitere Berechnung von Geldbußen zwischen den Aufsichtsbehörden harmonisieren und die bestehende Leitlinie der ehe-

³⁷ Siehe hierzu https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de?f%5B0%5D=opinions_date%3A2022&f%5B1%5D=opinions_publication_type%3A64

maligen Artikel-29-Datenschutzgruppe (WP253) ergänzen. Bei der Festlegung des „Ausgangsbetrags“ werden insbesondere drei Elemente berücksichtigt: die Kategorisierung der Verstöße nach ihrer Art, die Schwere des Verstoßes und der Umsatz eines Unternehmens. Der Anwendungsbereich der Leitlinien wurde auf die Berechnung von Geldbußen, die gegen juristische Personen verhängt werden, beschränkt. Für natürliche Personen gilt die Leitlinie nur dann, wenn sie als Unternehmen bzw. „undertaking“ agieren.

- zum Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung (5/2022, 12. Mai 2022): In dieser Leitlinie weist der EDSA darauf hin, dass der Einsatz von Gesichtserkennungstechnologie ernsthafte Risiken für die Rechte der betroffenen Personen in Bezug auf die Einhaltung des Gesetzes über die Verarbeitung personenbezogener Daten mit sich bringen könne und dass dies zu mehreren möglichen Verstößen gegen die Grundrechtecharta durch die Mitgliedstaaten bei der öffentlichen Nutzung solcher Technologien führen könnte. Der EDSA bekräftigt und erkennt die Bedeutung des Einsatzes solcher Instrumente für Sicherheitsfragen an, fordert jedoch, dass vor dem Einsatz von Gesichtserkennungstechnologie eine Bewertung der Erforderlichkeit und der Verhältnismäßigkeit vorgenommen werden müsse. Dabei wird die Forderung nach einem Verbot des Einsatzes von Gesichtserkennungstechnologien in bestimmten Fällen, wie etwa die Verwendung von Gesichtserkennungssystemen, die Personen auf der Grundlage ihrer biometrischen Daten in Gruppen nach ethnischer Zugehörigkeit, Geschlecht, politischer oder sexueller Orientierung oder anderen Diskriminierungsgründen einteilen oder um auf die Emotionen einer natürlichen Person zu schließen, wiederholt.
- zur praktischen Umsetzung der gütlichen Einigung (6/2022, 12. Mai 2022): Das Ziel dieser Leitlinie ist es, ein zufriedenstellendes Ergebnis für betroffene Personen zu erzielen, die Opfer einer Datenschutzverletzung geworden sind und sicherzustellen, dass die für die Datenverarbeitung Verantwortlichen die DSGVO einhalten. Um dieses Ziel zu erreichen, werden in den Leitlinien Best-Practice-Verfahren beschrieben, die eine einheitliche Anwendung der DSGVO sowohl auf EU- als auch auf nationaler Ebene bei Beschwerden betroffener Personen ermöglichen.
- zur Zertifizierung als Instrument für den Transfer (7/2022, 30. Juni 2022): Art. 46 Abs. 2 lit. f DSGVO führt einen genehmigten Zertifizierungsmechanismus als neues Instrument für die Übermittlung personenbezogener Daten in Drittländer ein, wenn kein Angemessenheitsabkommen besteht. Die Leitlinie ergänzt die Leitlinie 1/2018 zur Zertifizierung, die allgemeinere Hinweise zur Zertifizierung enthalten, und haben den Hauptzweck, die praktische Anwendung dieses Übermittlungsinstruments zu erläutern.
- zur Ermittlung der federführenden Aufsichtsbehörde eines für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters (8/2022, 10. Oktober 2022): Hierbei handelt es sich um eine aktualisierte Version der Leitlinie. Der EDSA hatte festgestellt, dass insbesondere hinsichtlich des Begriffs der „Hauptniederlassung“ im Zusammenhang mit der gemeinsamen Verantwortlichkeit und unter Berücksichtigung der Leitlinie 07/2020 weiterer Klärungsbedarf besteht. Nunmehr wurde klargestellt, dass der Begriff Hauptniederlassung sich auf einen einzigen Verantwortlichen beziehe und nicht auf die Situation einer gemeinsamen Verantwortlichkeit angewendet werden könne. Die Hauptniederlassung eines Verantwortlichen könne nicht als Hauptniederlassung für die gemeinsame Verantwortlichkeit gelten. Daher können gemeinsame

Verantwortliche auch keine gemeinsame Hauptniederlassung benennen.

- zur Meldung von Verletzungen des Schutzes personenbezogener Daten nach der DS-GVO (9/2022, 10. Oktober 2022): Hierbei handelt es sich um eine aktualisierte Version der Leitlinie WP250 rev.01. Dabei wird klargestellt, dass ein Verantwortlicher, der über keine Niederlassung im EWR-Raum verfügte, die Meldung betreffend eine Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde jenes Mitgliedstaates zu richten habe, in welchem sich betroffenen Personen aufhalten, unabhängig davon in welchem Mitgliedstaate sich der Art. 27-Vertreter befindet.

Darüber hinaus wurden auch folgende *Erklärungen*³⁸ des EDSA zu folgenden Themen angenommen:

- zum Antrag auf Genehmigung und zu den Elementen und Grundsätzen, welche in verbindlichen internen Datenschutzvorschriften für Verantwortliche (BCR-C) enthalten sein sollten (1/2022, 14. November 2022, in öffentlicher Konsultation): Diese Empfehlungen stellen eine Aktualisierung und Zusammenfügung der bestehenden BCR-C Dokumente (WP256, WP264) dar und bringen diese mit den Anforderungen des EuGH Urteils zu Schrems II in Einklang. Die Empfehlungen bieten eine zusätzliche Orientierungshilfe und sollen gleiche Wettbewerbsbedingungen für alle BCR-Antragsteller gewährleisten. Weitere Empfehlungen für Auftragsverarbeiter (BCR-P) werden erarbeitet.
- zur potenziellen Gestaltung des digitalen Euro unter dem Gesichtspunkt des Schutzes der Privatsphäre und des Datenschutzes (4/2022, 10. Oktober 2022): Im Juli 2021 beschloss die Europäische Zentralbank (EZB) eine 24-monatige Untersuchungsphase für einen möglichen digitalen Euro einzuleiten. In seiner Erklärung schlägt der EDSA die Einführung einer „Datenschutzschwelle“ vor, die als Transaktionswert ausgedrückt werde und bis zu dem keine Rückverfolgung der Transaktionen erfolgen dürfe. Darüber hinaus empfiehlt der EDSA in Hinblick auf den digitalen Euro einen spezifischen Rechtsrahmen für den Schutz personenbezogener Daten bei digitalen Zahlungen zu entwickeln.
- zu den Auswirkungen des EuGH-Urteils C-817/19 betreffend die Umsetzung der Richtlinie (EU) 2016/681 über die Verwendung von PNR-Daten (Anm: Passenger Name Record-Daten, Fluggastdatensätze) in den Mitgliedstaaten (5/2022, 15. Dezember 2022): In seinem Urteil vom 21. Juni 2022 führte der EuGH aus, dass die Gültigkeit der PNR-Richtlinie zwar nicht beeinträchtigt werde, die PNR-Richtlinie jedoch so ausgelegt werden müsse, dass sie wichtige Beschränkungen für die Verarbeitung personenbezogener Daten enthalte, um die Einhaltung der Grundrechtecharta zu gewährleisten. Einige dieser Einschränkungen seien die Anwendung des PNR-Systems nur auf terroristische Straftaten und schwere Kriminalität, die in einem objektiven Zusammenhang mit der Beförderung von Fluggästen stünden, und die nichtdiskriminierende Anwendung der allgemeinen Aufbewahrungsfrist von fünf Jahren auf alle personenbezogenen Daten von Fluggästen. Die vom EuGH vertretene Auslegung schränke die Möglichkeiten der Mitgliedstaaten zur Verarbeitung von Fluggastdaten erheblich ein. Der EDSA halte es daher für wahrscheinlich, dass die derzeitige Verarbeitung von PNR-Daten in vielen, wenn nicht gar den meisten Mitgliedstaaten nicht vollständig

³⁸ Siehe hierzu https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de?f%5B0%5D=opinions_date%3A2022&f%5B1%5D=opinions_publication_type%3A98

mit der PNR-Richtlinie in der Auslegung des EuGHs übereinstimme. PNR-Systeme in der gesamten EU könnten daher weiterhin tagtäglich in unverhältnismäßiger Weise in die Grundrechte der Betroffenen eingreifen. In seiner Erklärung fordert der EDSA die Mitgliedstaaten daher auf, alle notwendigen Schritte auf legislativer und/oder administrativer Ebene zu unternehmen, um sicherzustellen, dass ihre jeweilige nationale Umsetzung und Durchführung der PNR-Richtlinie im Einklang mit der Grundrechtecharta in der Auslegung des EuGHs steht. In diesem Zusammenhang weist der EDSA darauf hin, dass die Aufsichtsbehörden uneingeschränkt befugt seien, die Einhaltung der Datenschutzanforderungen der Union auf nationaler Ebene zu prüfen.

Im Oktober 2020 hatte der EDSA die Einrichtung eines koordinierten Durchsetzungsrahmens („Coordinated Enforcement Action“ - CEF) beschlossen, um den Vollzug und die Zusammenarbeit zwischen Aufsichtsbehörden im Einklang mit der EDPB-Strategie 2021-2023 zu gewährleisten. Als erstes Thema wurde „die Nutzung der Cloud im öffentlichen Sektor“ ausgewählt. Im Laufe des Jahres 2022 leiteten 22 Datenschutzbehörden im gesamten EWR (einschließlich des EDSB) koordinierte Untersuchungen (unter Verwendung einheitlicher Fragebögen) über die Nutzung von Cloud-basierten Diensten in ausgewählten Bereichen des öffentlichen Sektors ein. Insgesamt wurden rund 100 öffentliche Einrichtungen im gesamten EWR geprüft, darunter auch europäische Institutionen (wie Gesundheit, Finanzen, Steuern, Bildung, Käufer und Anbieter von IT-Diensten). Das amtswege Prüfverfahren der österreichischen Datenschutzbehörde hatte seinen Fokus im Bildungsbereich. Der gemeinsame Bericht³⁹ zu den Ergebnissen der durchgeführten Untersuchungen wurde am 17. Jänner 2023 durch den EDSA angenommen. Diesem ist etwa zu entnehmen, dass die am meisten genutzten Cloud Service Provider in den beteiligten EWR Staaten jene von Adobe, Amazon, Citrix, Google, Fujitsu, IBM, Microsoft, Oracle, OVH seien. Ein Abschnitt des Berichts ist der „Aushandlung maßgeschneiderter Verträge zwischen öffentlichen Einrichtungen und Cloud-Anbietern“ gewidmet, wobei diesfalls der Schluss gezogen wird, dass – sollten öffentliche Stellen aufgrund des Machtgefälles in der Praxis die Vertragsbedingungen nicht aushandeln können – der Cloud Service Anbieter uU als autonomer für die Verarbeitung Verantwortlicher im Sinne von Art. 28 Abs. 10 DSGVO betrachtet werden könne. Der Bericht enthält zudem eine Auflistung von Punkten, die bei Abschluss eines Vertrages mit einem Cloud Service Provider berücksichtigt werden sollten:

- Durchführung einer Datenschutzfolgenabschätzung;
- Klare und eindeutige Rollenfestlegung zwischen Cloud Service Provider und öffentlicher Stelle;
- Sicherstellen, dass der Cloud Service Provider nur im Namen und nach den dokumentierten Anweisungen der öffentlichen Stelle handelt und Identifizieren allfälliger Verarbeitungen, bei denen der Cloud Service Provider als Verantwortlicher agiert;
- Sicherstellen eines Widerspruchrechts gegen neue Sub-Auftragsverarbeiter;
- Festlegung, welche personenbezogene Daten für welche Zwecke verarbeitet werden;
- Einbindung des Datenschutzbeauftragten;
- Zusammenarbeit mit anderen öffentlichen Stellen bei Verhandlungen mit dem Cloud Ser-

39 Siehe hierzu https://edpb.europa.eu/news/news/2023/edpb-determines-privacy-recommendations-use-cloud-services-public-sector-adopts_en

vice Provider;

- Überprüfung, ob die Verarbeitung im Einklang mit der Datenschutzfolgenabschätzung erfolgt;
- Sicherstellen, dass bereits im Vergabeverfahren sämtliche notwendige Anforderungen zur DSGVO vorhanden sind;
- Identifizierung der Datenübermittlungen, die im Rahmen der routinemäßigen Erbringung von Dienstleistungen oder für eigene Zwecke des Cloud Service Providers stattfinden können, und Sicherstellung, dass dabei die Bestimmungen von Kapitel V der DSGVO eingehalten werden, notwendigerweise auch durch ergänzende Maßnahmen („supplementary measures“);
- Analyse, ob die Rechtsvorschriften eines Drittlandes, welche auf den Cloud Service Provider anwendbar sind, dazu führen können, dass öffentliche Stellen des Drittstaates Anträge auf Zugang zu Daten stellen können, selbst wenn diese vom Cloud Service Provider in der EU gespeichert wurden;
- Verträge mit Cloud Service Providern genau prüfen und gegebenenfalls neu aushandeln;
- Überprüfung der Bedingungen, unter denen die öffentliche Stelle zu Audits zugelassen ist bzw. dazu beitragen kann und sicherstellen, dass Audits vorhanden sind.

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 794/2016⁴⁰ 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.

Am 28. Juni 2022 trat eine Änderung der Europol Verordnung in Kraft⁴¹. Durch diese Verordnung wurden die Befugnisse von Europol im Hinblick auf die Verarbeitung großer Datensätze, den Austausch personenbezogener Daten mit privaten Akteuren, die Zusammenarbeit mit Drittländern und der Europäischen Staatsanwaltschaft, die Einleitung von Ermittlungen sowie im Bereich von SIS-Ausschreibungen erweitert. Zudem soll Europol die Mitgliedstaaten beim Einsatz von Technologien auf Grundlage künstlicher Intelligenz unterstützen. Weitere Ände-

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

41 <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R0991>

rungen betreffen die Zusammenarbeit der nationalen Kontrollbehörden der Mitgliedstaaten mit dem Europäischen Datenschutzbeauftragten. Der bisher dafür eingerichtete Beirat (Europol Cooperation Board) hat seine Arbeit eingestellt und wird diese nun von einem gemäß Art. 62 der Verordnung 2018/1725⁴² beim Europäischen Datenschutzausschuss (EDSA) eingerichteten Komitee (Coordinated Supervision Committee) fortgeführt. Hauptaufgabe des Komitees ist weiterhin, sich mit 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 Datenschutzbehörde als nationale Kontrollbehörde leitete im Jahr 2022 ein amtswegiges Prüfverfahren betreffend die vom Bundeskriminalamt im Bundesministerium für Inneres als nationale Europol-Stelle durchgeführten Datenübermittlungen an Europol ein. Das Verfahren ist derzeit noch anhängig.

6.1.3 Schengen (einschließlich Schengen Evaluierungen) sowie Visa

Das Schengener Informationssystem der zweiten Generation (kurz „SIS II“) ermöglicht nationalen Grenz-, Zoll-, Visa- und Strafverfolgungsbehörden Fahndungen zu gesuchten oder vermisste Personen bzw. gestohlene oder verlorene Sachen, insbesondere Dokumente und Fahrzeuge, im Schengen-Raum auszuschreiben bzw. abzufragen.

Die Rechtsgrundlage für das SIS II bildet die sogenannte SIS-II-Verordnung (Verordnung [EG] Nr. 1987/2006). 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 Visa-Informationssystem (kurz „VIS“) wiederum ist ein System für den Austausch von Visa-Daten zwischen den Mitgliedstaaten der Europäischen Union sowie assoziierten Ländern und enthält die Art des Visums, dessen Gültigkeitsdauer, allfällige Ablehnungen bzw. Annulierungen oder Aufhebungen von Visa sowie Identifikationsdaten. Dies ermöglicht den Behörden in ihrem Hoheitsgebiet die Echtheit von Visa zu überprüfen bzw. festzustellen, ob eine Person die Voraussetzungen für die Einreise oder den Aufenthalt im Hoheitsgebiet des Mitgliedstaats erfüllt.

Die Rechtsgrundlage für das VIS bildet die sogenannte VIS-Verordnung (Verordnung [EG] Nr. 767/2008). Das VIS besteht aus einem zentralen System (C.VIS), den jeweiligen nationalen Systemen der Mitgliedstaaten (N.VIS) sowie einer Kommunikationsinfrastruktur zwischen dem zentralen System und den nationalen Systemen.

Die jeweiligen nationalen Datenschutzbehörden haben gemäß der SIS-II-Verordnung bzw. der VIS-Verordnung die Rechtmäßigkeit der Verarbeitung personenbezogener SIS-II-Daten bzw. VIS-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 bzw. VIS-Verordnung in den einzelnen Mitgliedstaaten. Im November 2020 wurde die österreichische Datenschutzbehörde hinsichtlich der praktischen Umsetzung der relevanten Bestimmungen der SIS-II-Verordnung bzw. der VIS-Verordnung in ihrem Bereich überprüft. Mit Durchführungsbeschluss des Rates der Europäischen Union vom 17. Juni 2022 zur

42 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>

Zl. 10396/22⁴³ zur Beseitigung der im Jahr 2020 bei der Evaluierung festgestellten Mängel, ergingen acht Empfehlungen an die Datenschutzbehörde, wobei im Berichtszeitraum bereits sechs der acht Empfehlungen umgesetzt wurden.

Das laufende nationale N.SIS II Audit steht kurz vor dem Abschluss. Im Herbst 2023 wird ein neuerliches N.VIS Audit von der Datenschutzbehörde initiiert werden.

Darüber hinaus haben im Berichtszeitraum Mitarbeiter der Datenschutzbehörde an den Schengen-Evaluierungen der Länder Luxemburg, Norwegen und Island teilgenommen. Die Datenschutzbehörde wird sich auch im Jahr 2023 an Schengen-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-Verordnung⁴⁴ („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. Zukünftig sollen diese Aufgaben von einem bereits beim Europäischen Datenschutzausschuss (EDSA) gemäß Art. 62 der Verordnung 2018/1725⁴⁵ eingerichteten Komitee (Coordinated Supervision Committee) übernommen werden, sobald dies in den entsprechenden EU-Rechtsakten vorgesehen ist und diese in Kraft getreten sind. Der genaue Zeitpunkt hierfür steht noch nicht fest.

43 <https://data.consilium.europa.eu/doc/document/ST-10396-2022-INIT/en/pdf>

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

45 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>

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. 603/2013⁴⁶ 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. Zu diesem Zweck wurde die Eurodac Supervision Coordination Group („Coordination Group“) gebildet. Zukünftig sollen diese Aufgaben von einem bereits beim Europäischen Datenschutzausschuss (EDSA) gemäß Art. 62 der Verordnung 2018/1725⁴⁷ eingerichteten Komitee (Coordinated Supervision Committee) übernommen werden, wobei der Zeitpunkt für den Übergang der Aufgaben noch nicht feststeht.

6.2 Europarat

Die Datenschutzbehörde vertritt die Republik Österreich im Ausschuss nach Art. 18 (T-PD) der Datenschutzkonvention des Europarates (EVS Nr. 108, BGBl. Nr. 317/1988). Im Berichtszeitraum fand von 16. bis 18. November 2022 die 43. 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.

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

47 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>

7 Internationale Beziehungen

Auch im Jahr 2022 fand die Konferenz der Internationalen Datenschutzversammlung (Global Privacy Assembly - GPA)⁴⁸ statt. Die GPA ist seit mehr als vier Jahrzehnten ein wichtiges globales Forum für Aufsichtsbehörden im Datenschutzbereich.

Die Global Privacy Assembly (GPA) „A Matter of Balance. Privacy in The Era of Rapid Technological Advancement“ (Datenschutz im Zeitalter des rasanten technologischen Fortschritts) wurde von der türkischen Aufsichtsbehörde vom 25. bis 28. Oktober 2022 in Istanbul im hybriden Rahmen abgehalten, wobei die offene Sitzung vom 25. bis 26. Oktober 2022 und die geschlossene Sitzung vom 27. bis 28. Oktober 2022 stattfanden.

Die Vorträge und Diskussionen der offenen Sitzung konzentrierten sich auf die technologischen Entwicklungen im Bereich der Gesichtserkennung, der Künstlichen Intelligenz und der Blockchain und deren Herausforderungen für den Datenschutz, aber auch auf den grenzüberschreitenden Datentransfer sowie auf Datenschutzrisiken im Bereich der humanitären Hilfe und für besondere schutzbedürftige Gruppen wie Kinder.

Die Leiterin der französischen Aufsichtsbehörde und der deutsche Bundesdatenschutzbeauftragte hielten gemeinsam eine Grundsatzrede zur „Konvergenz der Datenschutzbestimmungen bei grenzüberschreitenden Datenübermittlungen“. Mehrere Vertreter des EDSA nahmen an verschiedenen Diskussionsveranstaltungen teil. Der Europäische Datenschutzbeauftragte moderierte die Diskussionsrunde „Effizienz der für grenzüberschreitende Datenübermittlungen entwickelten Mechanismen“, die Vorsitzende des EDSA das Penal „Interaktion zwischen Verbraucherrechten, Wettbewerb und Datenschutz“.

Während der offenen Sitzung wurde Elizabeth Denham, ehemalige Leiterin der britischen Aufsichtsbehörde und ehemalige Vorsitzende des GPA, mit dem „Giovanni Buttarelli Award“ ausgezeichnet.

In der geschlossenen Sitzung berichteten die GPA-Arbeitsgruppen, der Unterausschuss für die strategische Ausrichtung des GPA und verschiedene GPA-Mitglieder und Beobachter sowie die Berliner Gruppe und andere Partnerorganisationen der Versammlung. Die Grundsatzreferate und Diskussionen während der Klausurtagung konzentrierten sich auf die Verbesserung der Effizienz und die Stärkung der Zusammenarbeit der internationalen Aufsichtsbehörden.

Darüber hinaus wurden nachstehende Resolutionen angenommen:

- Entschließung zur Änderung des Fahrplans und des Zeitplans für die Einrichtung eines finanzierten Sekretariats der GPA,
- Entschließung zum Aufbau von Kapazitäten für die internationale Zusammenarbeit zur Verbesserung der Regulierung der Cybersicherheit und zum Verständnis der durch Cybervorfälle verursachten Schäden,
- Entschließung zu den Grundsätzen und Erwartungen für die angemessene Nutzung personenbezogener Daten in der Gesichtserkennungstechnologie (Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology).

48 Siehe hierzu <https://globalprivacyassembly.org/>

Während der geschlossenen Sitzung des GPA erhielt die dänische Aufsichtsbehörde nach einer Abstimmung der Versammlung sowohl den Preis für „Bildung und öffentliches Bewusstsein“ als auch den „People's choice“ Award für „Datadysten“, ein speziell für Kinder und Jugendliche entwickeltes Spiel.

Die Aufsichtsbehörde der Bermudas wird die Konferenz im Jahr 2023 ausrichten.