dsb

Republik Österreich

Datenschutz behörde

Datenschutzbericht 2024

Datenschutzbericht 2024

Wien, im März 2025

Republik Österreich
Datenschutz
behörde

Impressum

Medieninhaber, Herausgeber und Redaktion:
Datenschutzbehörde, Dr. Matthias Schmidl
(gemäß § 18 ff DSG), Barichgasse 40-42, 1030 Wien
Kontakt: dsb@dsb.gv.at
Website: www.dsb.gv.at
Fotonachweis: Sebastian Freiler (Seite 5)
Gestaltung: Datenschutzbehörde
Druck: BMJ
Wien, 2025

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABl.	Amtsblatt
Abs.	Absatz
Art.	Artikel
AVG	Allgemeines Verwaltungsverfahrensgesetz
BGBl.	Bundesgesetzblatt
BGStG	Bundes-Behindertengleichstellungsgesetz
BlgNR	Beilage(-n) zu den Stenographischen Protokollen des Nationalrates
bspw.	beispielsweise
B-VG	Bundes-Verfassungsgesetz
BVwG	Bundesverwaltungsgericht
bzgl.	bezüglich
d.h.	das heißt
DSB	Datenschutzbehörde
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
DSRL-PJ	Datenschutzrichtlinie für den Bereich Polizei und Justiz
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
ErwGr.	Erwägungsgrund
EU	Europäische Union
EU-GRC	Charta der Grundrechte der Europäischen Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
FMA	Finanzmarktaufsicht
FN	Fußnote
GewO	Gewerbeordnung
IFG	Informationsfreiheitsgesetz
IO	Insolvenzordnung
iSd.	Im Sinne der/des
iVm.	In Verbindung mit
JN	Juristiktionsnorm
KDD-G	Koordinator-für-digitale-Dienste-Gesetz
KI	Künstliche Intelligenz
KI-VO	Verordnung über Künstliche Intelligenz
lit.	litera (-ae)
LG	Landesgericht
LVwG	Landesverwaltungsgericht
MedienG	Mediengesetz
mwN	mit weiteren Nachweisen
Nr.	Nummer
OGH	Oberster Gerichtshof
ORF-G	ORF-Gesetz

• PartG	Parteiengesetz
• RIS	Rechtsinformationssystem
• Rz.	Randziffer
• SPG	Sicherheitspolizeigesetz
• StGB	Strafgesetzbuch
• TKG	Telekommunikationsgesetz
• VfGH	Verfassungsgerichtshof
• VfSlg.	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des Verfassungsgerichtshofes
• vgl.	vergleiche
• VwGH	Verwaltungsgerichtshof
• VwSlg.	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des Verwaltungsgerichtshofes
• WAG	Wertpapieraufsichtsgesetz
• Z	Ziffer

1. Vorwort

Sehr geehrte Leserinnen und Leser!

Der vorliegende Datenschutzbericht des Jahres 2024 ist der zweite, den ich in meiner Funktion als Leiter der DSB zur Gänze verantworten darf.

Das Jahr 2024 war ein sehr ereignisreiches und bedeutsames Jahr für die DSB.

Eingeleitet wurde es durch ein Urteil des EuGH am 16. Jänner 2024[1] , welches zur Folge hatte, dass der Gesetzgeber eine zweite Datenschutz-Aufsichtsbehörde in Österreich einrichtete – das **Parlamentarische Datenschutzkomitee**.

Somit gibt es mit Wirkung vom 1. Jänner 2025 erstmals in der Geschichte des österreichischen Datenschutzes zwei Aufsichtsbehörden, welche ihre Tätigkeiten aufeinander abzustimmen haben werden.

Aufgrund eines Erkenntnisses des VfGH war der Gesetzgeber außerdem dazu angehalten, das so genannte „**Medienprivileg**“ in **§ 9 DSG** zu novellieren. Auch dies erfolgte im Berichtszeitraum.

Die DSB hat im Jahr 2024 zudem ihre **bilateralen Kontakte** zu den Datenschutz-Aufsichtsbehörden der unmittelbaren Nachbarschaft und darüber hinaus vertieft. Eine vertrauensvolle Kooperation innerhalb der EU aber auch mit bestimmten Drittstaaten - allen voran die **Schweiz** - ist für eine effektive Durchsetzung der DSGVO essentiell. In diesem Zusammenhang war es der DSB ein Anliegen, die Datenschutz-Aufsichtsbehörde des **Kosovo** in **zwei EU-finanzierten Projekten** zu unterstützen und diese somit näher an den Rechtsbestand und den Standard der EU heranzuführen.

Im **EDSA** wirkt die DSB seit jeher sehr aktiv mit, was sich im Berichtszeitraum auch nicht änderte.

Nicht nur im Bereich des Datenschutzes sind Kooperationen wichtig, sondern auch mit inländischen Behörden und Einrichtungen. Im Berichtsjahr wurde die Erklärung über ein „**Netzwerk Digitalisierung**“ unterfertigt. Die DSB ist Teil dieses inländischen Netzwerks, das verschiedene unabhängige Aufsichts- und Regulierungsbehörden verbindet.

Ebenso ging die DSB aktiv auf die gesetzlichen Interessensvertretungen zu.

Neben all diesen Tätigkeiten lag der Fokus der DSB – wie gewohnt – auf ihren **Kernaufgaben,** nämlich der Wahrnehmung der ihr von der DSGVO und dem DSG übertragenen Aufgaben, wobei der Sensibilisierung für Datenschutzfragen in Form von **Rundschreiben und Vorträgen** besondere Bedeutung beigemessen wurde.

Die **Arbeitsbelastung** insgesamt, aber auch pro Kopf, ist dabei **anhaltend hoch** und die **Erhöhung des Personalstandes somit unausweichlich**, wenn die DSB weiterhin ihren Aufgaben nachkommen können soll. Derzeit ist dies nur möglich, indem Schwerpunkte in zeitlich

1 Urteil des EuGH vom 16. Jänner 2024, Rs. C-33/22, https://curia.europa.eu/juris/liste.jsf?language=de&num=C-33/22.

festgelegten Fenstern gesetzt werden, was die Vernachlässigung anderer Aufgaben in diesem Zeitraum zur Folge hat.

Eine Aufstockung des Personalstandes ist auch deshalb dringend erforderlich, weil sowohl der nationale, als auch der Unionsgesetzgeber der DSB zusätzlich Aufgaben übertragen.

Zusätzliche Aufgaben erfordern zusätzliche Mittel!

Zu erwähnen sind hier das **IFG**, die **KI-VO**, die **Verordnung über die Transparenz und das Targeting politischer Werbung** und die **NIS 2-Richtlinie**. Auf all diese Vorgaben wird im vorliegenden Datenschutzbericht näher eingegangen.

Zuletzt möchte ich erwähnen, dass die Webseite der DSB von Grund auf erneuert wurde und seit Dezember 2024 in einem neuen Licht erstrahlt. Ich lade Sie herzlich ein, die Webseite zu besuchen.

Ich wünsche Ihnen bei der Durchsicht viel Freude und hoffe, dass Sie die dargestellten Informationen nützlich und interessant finden.

Dr. Matthias Schmidl, Leiter der DSB

2. Die Datenschutzbehörde

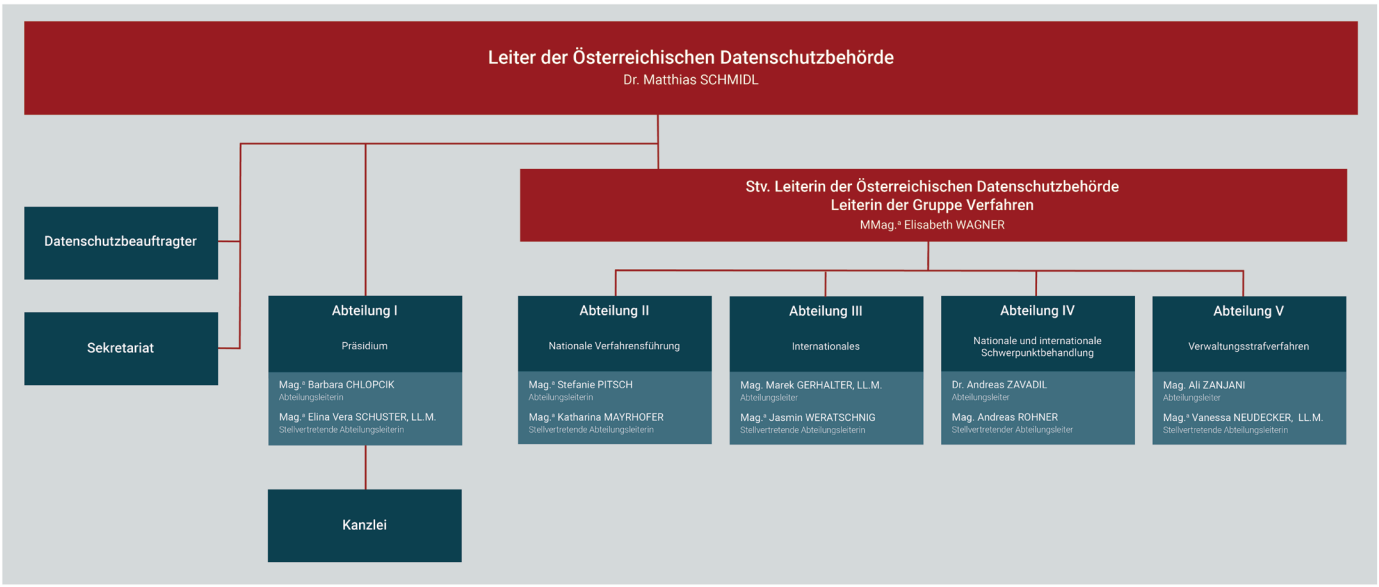
2.1 Organisation und Aufgaben

2.1.1. Die Datenschutzbehörde

Die DSB ist **monokratisch** strukturiert, aufgrund europarechtlicher und völkerrechtlicher Vorgaben unabhängig und **keiner Dienst- und Fachaufsicht unterworfen**. Die Funktion des Leiters wird seit 1. Jänner 2024 von **Dr. Matthias Schmidl**, jene der stellvertretenden Leiterin von **MMag. Elisabeth Wagner** wahrgenommen.

Seit dem Jahr 2023 gliedert sich die DSB in **5 Abteilungen**, die jeweils von einer Abteilungsleiterin bzw. einem Abteilungsleiter geführt werden. Die stellvertretende Behördenleiterin hat zusätzlich die Leitung der Gruppe Verfahren inne.

Organigramm: Österreichische Datenschutzbehörde (DSB)
Stand: November 2024



Die Abteilungsleiter:innen sind Dienst- und Fachvorgesetzte der jeweiligen Bediensteten und entlasten durch diese Leitungstätigkeit den Leiter und die stellvertretende Leiterin der DSB.

Durch die **Spezialisierung der Abteilungen** ist es möglich, Aufgaben zielgerichtet zuzuweisen und zu bearbeiten.

Trotz der notwendigen Spezialisierung legt die DSB großen Wert darauf, dass die einzelnen Bediensteten möglichst „breit“ aufgestellt sind, dh. über eine entsprechende Wissenspalette im Datenschutzrecht und in verwandten Rechtsgebieten verfügen, die einen Einsatz in jeder Abteilung ermöglicht. Als Grundsatz ist jede:jeder Bedienstete zwei Abteilungen zugewiesen.

Auf diese Weise wird die notwendige Flexibilität gewährleistet, die erforderlich ist, um Arbeitsspitzen abzudecken. Gleichzeitig hat sich eine breite Aufstellung im internationalen Vergleich als vorteilhaft erwiesen, weil jene Bediensteten, die in den Untergruppen des EDSA tätig sind, über fundiertes Wissen in der Führung von Verfahren verfügen und somit zu praktikablen Ergebnissen beitragen können. Lediglich die Führung von Verwaltungsstrafverfahren wird von Bediensteten wahrgenommen, die keiner weiteren Verfahrensabteilung zugewiesen sind. Dadurch soll verhindert werden, dass es zu Überschneidungen bei der Führung von Verwaltungs- und Verwaltungsstrafverfahren gegen idente Verantwortliche und Auftragsverarbeiter kommt und gewährleistet werden, dass Verwaltungsstrafverfahren somit unvoreingenommen geführt werden können.

2.1.2 Aufgaben und Befugnisse nach der DSGVO und dem DSG

Sämtliche Aufgaben der Datenschutzbehörde sind in **Art. 57 DSGVO** normiert:

- 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 EDSA
- 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 EDSA
- 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 EDSA
- Genehmigung von Zertifizierungskriterien (Art. 42 DSGVO) sowie die Erlassung der korrespondierenden Verordnung über die Akkreditierung von Zertifizierungsstellen (Art. 43 DSGVO) unter Einbindung des EDSA
- Die Genehmigung von verbindlichen internen Vorschriften (BCR) sowie von Vertragsklauseln zur Übermittlung von Daten an Empfänger in Drittstaaten oder internationale Organisationen (Art. 46 f DSGVO) unter Einbindung des EDSA

- 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 EDSA (Art. 63 ff DSGVO)

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

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

Alle Bescheide der DSB können mit **Beschwerde an das BVwG** bekämpft werden. Dieses entscheidet im Dreiersenat (ein Berufsrichter, zwei Laienrichter). Entscheidungen des BVwG können – auch von der DSB – mit Revision an den VwGH bzw. Beschwerde an den VfGH bekämpft werden.

Die DSB stellt auf der **Website** der DSB a**llgemeine Informationen zu den Verfahren vor der DSB** sowie **Musterformulare** für Eingaben zur Verfügung. Seit Dezember 2024 existiert eine grundlegend überarbeitete Webseite mit zusätzlichen Informationen und **neuen Online-Formularen**. Dabei wurde besonders Wert auf eine leichte Auffindbarkeit relevanter Informationen gelegt.

Die wichtigsten Entscheidungen der DSB werden im **RIS** veröffentlicht. Die DSB ist dazu übergegangen, auch dann Entscheidungen zu veröffentlichen, wenn diese noch nicht rechtskräftig sind, aber relevante Informationen enthalten. Nicht rechtskräftige Entscheidungen sind durch einen entsprechenden Hinweis ausgewiesen.

2.1.3 Aufgaben nach dem IFG

Gemäß **§ 15 Abs. 1 IFG** berät und unterstützt die DSB die informationspflichtigen Organe bzw. Einrichtungen durch die Bereitstellung von Leitfäden und Angebote zur Fortbildung in datenschutzrechtlichen Belangen der Vollziehung der Informationsfreiheit.

Abs. 2 dieser Bestimmung überträgt der DSB die Aufgabe, die Anwendung des IFG begleitend zu evaluieren und die Öffentlichkeit über ihre Tätigkeiten zu informieren.

Das IFG wurde im Berichtszeitraum kundgemacht (BGBl. I Nr. 5/2024) und tritt überwiegend mit **1. September 2025 in Kraft**. Um ihren Aufgaben nachzukommen, hat die DSB bereits im Jahr 2024 erste Maßnahmen gesetzt, auf welche in **Kapitel 3.3.** näher eingegangen wird.

Die Aufgaben nach dem IFG berühren nicht die Aufgaben und Befugnisse nach der DSGVO und dem DSG.

2.1.4 Aufgaben nach der KI-VO

Die Verordnung über künstliche Intelligenz (Verordnung (EU) 2024/1689) wurde im Berichtszeitraum im ABl. kundgemacht (ABl. Nr. L 2024/1689 vom 12. Juli 2024) und wird in den Folgejahren schrittweise in Geltung treten.

Im Berichtszeitraum wurde die **DSB als Grundrechtsbehörde nach Art. 77 KI-VO** der Europäischen Kommission notifiziert (Art. 77 Abs. 2 KI-VO).

Auf die KI-VO wird in **Kapitel 3.4.** näher eingegangen.

Auch diese Aufgabe berührt nicht die Aufgaben und Befugnisse nach der DSGVO und dem DSG.

2.1.5 Aufgaben nach der Verordnung über die Transparenz und das Targeting politischer Werbung

Diese Verordnung (Verordnung (EU) 2024/900) wurde ebenso im Berichtszeitraum im ABl. kundgemacht (ABl. Nr. L 2024/900 vom 30. März 2024) und **gilt ab dem 10. Oktober 2025**.

Punktuell überträgt diese Verordnung den Datenschutz-Aufsichtsbehörden Aufgaben und Befugnisse, worauf in **Kapitel 3.5.** näher eingegangen wird.

Auch diese Aufgabe berührt nicht die Aufgaben und Befugnisse nach der DSGVO und dem DSG.

2.2 Der Personalstand

Ende des Jahres 2024 arbeiteten **72 Bedienstete** in der DSB. Dies entspricht **50,00 Vollbeschäftigungsäquivalenten (VBÄ)**, unter Einbeziehung dreier nach dem Behindertenteinstellungsgesetz besetzten Stellen sowie **19 Verwaltungspraktikant:innen**. Neun der Praktikant:innen waren dem juristischen Dienst und zehn dem gehobenen Dienst zuzuordnen (davon neun des gehobenen Dienstes mit einem Beschäftigungsausmaß von 50 %).

3. Allgemeine Erfahrungen der DSB im Berichtszeitraum, einschließlich Parlamentarischer Anfragen

3.1 Allgemeine Erfahrungen der Datenschutzbehörde, einschließlich Personalausschuss

3.1.1. Hohe Verfahrenszahlen gepaart mit einem zu niedrigen Personalstand

Auch wenn der Personalstand in den letzten Jahren, dank des Einsatzes der Bundesministerin für Justiz, Dr. Alma Zadić, nachhaltig gestiegen ist, ist er in Relation zur Zahl der anhängigen Verfahren nach wie vor in Summe zu niedrig. Darauf wurde bereits im Datenschutzbericht 2023 hingewiesen.

Die Auswertung für Dezember 2024 ergibt, dass **eine:ein juristische:r Bedienstete im Schnitt** nach wie vor **mit mehr als 100 Verfahren belastet** ist, was eine zielgerichtete und vor allem zeitgerechte Bearbeitung faktisch unmöglich macht.

Zur Verfahrensführung hinzu kommen noch die anderen, in Art. 57 DSGVO aufgezählten Aufgaben, insbesondere die Begutachtung von Gesetzes- und Verordnungsentwürfen sowie die Mitarbeit im EDSA.

Seit dem Jahr 2017 ist allein im Bereich der **Individualbeschwerden** eine **Steigerung von 769%** zu verzeichnen. Legt man diesen Anstieg auf die Anzahl der Bediensteten um, müsste der Personalstand der DSB bei 189 Bediensteten liegen, was einer Verdreifachung des derzeitigen Personalstandes entspräche!

Abgesehen davon werden zusätzliche Aufgaben aufgrund bundesgesetzlicher oder unionsrechtlicher Vorgaben der DSB übertragen werden.

Trotz dieser Entwicklung ist die DSB handlungsfähig und kommt ihren Verpflichtungen im Rahmen des Möglichen nach. Sollte jedoch keine Aufstockung des Personalstandes erfolgen, ist davon auszugehen, dass die DSB den ihr übertragenen Aufgaben nicht mehr nachkommen kann, ohne andere Aufgaben zu vernachlässigen.

3.1.2. Maßnahmen zur Effizienzsteigerung

Zur Steigerung der Effizienz wurde im Berichtsjahr ein „**Erstsichtungssystem**“ eingeführt.

Im Rahmen einer solchen Erstsichtung werden sämtliche externe Eingaben an die DSB mit einer Anregung, dass von Amts wegen ein Sachverhalt ermittelt und in Folge Abhilfebefugnisse nach **Art. 58 Abs. 2 DSGVO** ergriffen werden sollen, von speziell hierfür eingesetzten Mitarbeiter:innen unter der Leitung der Abteilung V. gesichtet. Konkret wird hierbei geprüft, ob (1) es sich zunächst überhaupt um eine substantiierte Anzeige handelt, (2) ein für die DSB

relevanter Verstoß erblickt werden kann und (3) gemessen daran ein Anfangsverdacht für ein Ermittlungsverfahren besteht. In weiterer Folge werden nur jene Eingaben an die zuständige Abteilung weitergeleitet, die von der DSB von Amts wegen behandelt und einem Ermittlungsverfahren zugeführt werden sollen. Ansonsten werden die Eingaben vorab im Rahmen der Erstsichtung eingestellt und ohne weitere Maßnahmen abgelegt, sofern die Eingabe nicht zuständigkeitshalber an eine andere Behörde weiterzuleiten ist.

Im Zuge der Erstsichtung wird zudem geprüft, ob das Auslangen mit einem Sensibilisierungsschreiben der DSB (ohne Ermittlungsverfahren) gefunden werden kann. Mit einem solchen Sensibilisierungsschreiben weist die DSB Verantwortliche und/oder Auftragsverarbeiter:innen auf einen vermeintlichen Verstoß und die geltende Rechtslage hin (**Art. 58 Abs. 1 lit. d DSGVO**).

3.1.3. Verstärkung der bilateralen Kooperationen mit ausländischen Datenschutz-Aufsichtsbehörden

Im Berichtszeitraum hat die DSB gezielt Kontakt zu den Datenschutzaufsichtsbehörden der unmittelbaren Nachbarstaaten gesucht.

Im Juni 2024 erfolgte ein Besuch in Bern beim **Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten** (EDÖB). Auch wenn die Schweiz dem EWR nicht angehört, ist eine bilaterale Kooperation dennoch wichtig, da grenzüberschreitende Sachverhalte die Schweiz betreffen können und in diesem Fall der Kooperationsmechanismus nach der DSGVO nicht zur Anwendung gelangt.

Zudem verfügt der EDÖB über eine 20-jährige Erfahrung als „Informationsfreiheitsbehörde", was im Hinblick auf die Aufgaben, welche das IFG der DSB überträgt, einen nicht unwesentlichen Mehrwert darstellt. Aufgrund dieser bilateralen Kooperation war es möglich, dass der Leiter des Öffentlichkeitsbereichs des EDÖB die DSB im Rahmen der Auftaktveranstaltung zum IFG im September 2024 maßgeblich unterstützte.

Im September 2024 fand auf Initiative der DSB in Wien zudem ein Treffen der mitteleuropäischen Datenschutzaufsichtsbehörden – dh. aus **Tschechien**, der **Slowakei**, **Ungarn** und **Slowenien** – statt. Dieses Treffen war schon insofern ein Erfolg, als beschlossen wurde, dieses Format in den Folgejahren fortzuführen. Da die Datenschutzaufsichtsbehörden dieser Länder eine ähnliche Größe wie die DSB aufweisen und vor ähnlichen Herausforderungen stehen, ist der Austausch von Informationen und Erfahrungen sehr wichtig.

Mit der deutschen Bundes-Datenschutzaufsichtsbehörde (**Bundesbeauftragte für Datenschutz und Informationsfreiheit – BfDI**) sowie der Bayrischen Datenschutzaufsichtsbehörde für den öffentlichen Bereich (**Bayrischer Landesbeauftragter für Datenschutz – BayLfD**) und der Leiterin der **Datenschutzstelle in Liechtenstein** steht die DSB ebenso in einem vertieften und vertrauensvollen Austausch.

Darüber hinaus hat sich eine sehr gute Kooperation mit der **kroatischen Datenschutzaufsichtsbehörde** entwickelt, was auch daran liegt, dass der österreichischen und der kroatischen Datenschutzaufsichtsbehörde eine Unterstützung der **kosovarischen Datenschutzaufsichtsbehörde** ein wesentliches Anliegen ist. Zudem bekleidet der Leiter der kroatischen Datenschutzaufsichtsbehörde seit 2024 die Funktion des stellvertretenden Vorsitzenden des EDSA.

Näheres dazu ist dem **Kapitel 7** dieses Berichts zu entnehmen.

3.1.4. Parlamentarische Anfragen

Im Jahr 2024 wurden folgenden parlamentarische Anfragen, die die DSB betrafen, an die Bundesministerin für Justiz sowie die Bundesministerin für Klimaschutz gestellt:

- 17662/J und 17663/J betreffend Einzige Konsequenz des Klimarates: ein Prüfverfahren der Datenschutzbehörde

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 der Leiter 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.

3.1.5. Verstärkung der Kooperationen im Inland

Da Datenschutz erfahrungsgemäß dann respektiert und akzeptiert wird, wenn ein grundlegendes Verständnis dafür vorhanden ist, ist die DSB im Jahr 2024 gezielt auf die beruflichen Interessensvertretungen (**Wirtschaftskammer, Arbeiterkammer und Industriellenvereinigung**) zugegangen. Dies in der Absicht, in einen allgemeinen Austausch zu treten und das Verständnis für Datenschutz zu schärfen. Der DSB erscheint dies insofern wichtig, als diese Interessensvertretungen Informationen zum Datenschutz rasch an ihre Mitglieder weiterleiten und so für eine Verteilung „in der Fläche" sorgen können. Beispiele hiefür sind die **Rundschreiben der DSB zum Verhältnis zwischen Datenschutz und künstlicher Intelligenz,** welche auch auf der Webseite der DSB abrufbar sind.

Ein besonderes Anliegen war der DSB die Kooperation mit anderen (unabhängigen) Aufsichts- und Regulierungsbehörden in Österreich.

Die DSB hatte maßgeblichen Anteil daran, dass im November 2024 die **„Erklärung über ein Netzwerk Digitalisierung"** unterzeichnet wurde. Diesem Netzwerk gehören neben der DSB die **Bundeswettbewerbsbehörde**, die **e-control**, die **Finanzmarktaufsicht**, die **Kommunikationsbehörde Austria**, die **RTR GmbH** (Fachbereich Post und Telekom), die **Schienen Control GmbH** sowie die **Telekom-Control-Kommission** an.

Im Fokus steht dabei der **wechselseitige Informationsaustausch zu Themen der Digitalisierung** (vor allem künstliche Intelligenz), da diese Themen alle Behörden gleichermaßen betreffen und Auswirkungen auf alle Lebensbereiche haben. Diese Behörden haben unterschiedliche Ausrichtungen und verfügen über ein entsprechendes Fachwissen in verschiedenen Bereichen der Digitalisierung. Ein strukturierter Austausch von Informationen erspart unnötigen Zeitaufwand und vermeidet nach Möglichkeit unterschiedliche Entscheidungen. Die jeweilige verfassungs- und/oder unionsrechtlich garantierte Unabhängigkeit wird dadurch nicht berührt. Dieses Netzwerk zeigt, dass diese Behörden „über den Tellerrand" schauen, die Notwendigkeit eines vertieften Informationsaustausches erkannt haben und auch gewillt sind, im Interesse der Normunterworfenen zu kooperieren.

3.1.6. Vorabentscheidungsersuchen an den EuGH

Das Jahr 2024 war, ebenso wie die drei Jahre zuvor, von einer hohen Anzahl von an den EuGH gerichteten Vorabentscheidungsverfahren zur Auslegung der DSGVO gekennzeichnet.

In **14 Fällen** (2023: 24) richteten nationale (Höchst-)Gerichte Vorabentscheidungsersuchen an den EuGH. Darunter befinden sich auch **drei Vorabentscheidungsersuchen aus Österreich,** welche die DSB teilweise unmittelbar betreffen:

- **C-414/24,** eingereicht vom VwGH
- **C-468/24**, eingereicht vom LG St. Pölten sowie
- **C-474/24**, eingereicht vom BVwG

In 29 Fällen wurde im Berichtszeitraum eine Entscheidung verkündet (davon 24 Urteile aufgrund eines Vorabentscheidungsersuchens), darunter jenes vom 16. Jänner 2024 in der Rs. **C-33/22**, welches zur Einrichtung des Parlamentarischen Datenschutzkomitees führte.

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

Gleichzeitig ist festzustellen, dass die immer höhere Anzahl an Entscheidungen des EuGH zwar zur Rechtssicherheit beiträgt, jedoch in vielen Fällen eine Kasuistik aufweist, welche es erschwert, den Überblick zu behalten.

3.1.7. Beschwerden an die Volksanwaltschaft und andere Stellen

In **10 Fällen** wurde die DSB von der Volksanwaltschaft zur Stellungnahme aufgefordert, weil sich Beschwerdeführer:innen an sie gewendet hatten. Damit ist die Zahl im Vergleich zum Zeitraum 2023 (21 Beschwerden) gesunken, wobei auch im Jahr 2024 **allein 7 Beschwerden vom selben Beschwerdeführer** eingebracht wurden.

Ein Großteil dieser Beschwerden betraf die Verfahrensdauer vor der DSB.

In einem Fall musste sich die DSB im Rahmen eines Schlichtungsverfahrens gemäß **§ 14 BGStG** verantworten, weil ihr ein diskriminierendes Verhalten vorgeworfen worden war. Das Schlichtungsverfahren wurde zwar ohne Einigung beendet, eine Amtshaftungsklage in Folge aber nicht eingebracht.

3.1.8. Informationsfreiheit und künstliche Intelligenz

Auf diese Punkte wird im Detail in den **Kapiteln 3.3. und 3.4.** eingegangen werden.

Sowohl das IFG als auch die KI-VO wurden im Berichtszeitraum kundgemacht und normieren Zusatzaufgaben für die DSB.

Soweit es das IFG betrifft, kommt der DSB eine eingeschränkte Zuständigkeit zur Beratung und Schulung informationspflichtiger Stellen zu. Nach dem ausdrücklichen Willen des Gesetzgebers wird die DSB keine Informationsfreiheitsbehörde.

3.1.9. Reduktion von Verwaltungsstrafen durch das BVwG

Im Berichtszeitraum fiel auf, dass bei Beschwerdeverfahren in Verwaltungsstrafsachen durch das BVwG **in vielen Fällen eine (deutliche) Reduktion der von der DSB verhängten Verwaltungsstrafe** vorgenommen wurde.

In einem Fall wurde die von der DSB verhängte Verwaltungsstrafe in Höhe von 4 Millionen Euro auf 50 000 Euro reduziert.

Die Festlegung der Verwaltungsstrafe der DSB erfolgt anhand der vom EDSA beschlossenen einschlägigen Leitlinien, somit anhand objektiver Kriterien, an denen sich in aller Regel auch das BVwG orientiert.

Dennoch steht zu befürchten, dass die **generalpräventive Wirkung** von Geldstrafen in den Hintergrund tritt, wenn es zu einer deutlichen Reduktion der Geldstrafe kommt.

Die DSB bringt daher ausgewählte Fälle vor den VwGH, um Rechtssicherheit zu erlangen.

3.2. DSG-Novellen 2024

Im Jahr 2024 wurde das DSG zwei Mal novelliert, wobei für beide Novellen jeweils eine höchstgerichtliche Entscheidung ausschlaggebend war.

3.2.1. Das so genannte „Medienprivileg“

Mit Erkenntnis des VfGH vom 14. Dezember 2022, **G 287/2022 ua.**, wurde **§ 9 Abs. 1 DSG idF BGBl. I Nr. 24/2018 als verfassungswidrig aufgehoben**.

Nach Auffassung des VfGH widersprach der absolute und gänzliche – und damit undifferenzierte – Ausschluss der Anwendung aller (einfachgesetzlichen) Regelungen des DSG sowie näher bezeichneter Kapitel der DSGVO auf näher definierte Datenverarbeitungen zu journalistischen Zwecken eines Medienunternehmens oder Mediendienstes dem in § 1 Abs. 2 DSG normierten Erfordernis, dass der Gesetzgeber das Interesse am Schutz personenbezogener Daten mit dem Interesse der Medieninhaber:innen, Herausgeber:innen, Medienmitarbeiter:innen und Arbeitnehmer:innen eines Medienunternehmens oder Mediendienstes (im Sinne des Mediengesetzes) im Rahmen ihrer journalistischen Tätigkeit sachgerecht abzuwägen hat.

Mit der **Novelle BGBl. I Nr. 62/2024** wurde § 9 Abs. 1 DSG geändert und gleichzeitig ein **Abs. 1a** eingefügt. Die DSB gab dazu eine umfassende Stellungnahme ab (abrufbar unter https://www.parlament.gv.at/PtWeb/api/s3serv/file/6ff5a285-69a3-4e60-92f1-fa2863e7ccbd).

Ein pauschaler Ausschluss datenschutzrechtlicher Regelungen zugunsten der journalistischen Tätigkeit ist nunmehr nicht vorgesehen. Stattdessen sehen die **Z 1 bis Z 13 Ausnahmen vom Anwendungsbereich der DSGVO** vor.

Mit **§ 9 Abs. 1a DSG** wurde eine Regelung geschaffen, um den so genannten „**Bürgerjournalismus**“ (z.B. Blogger:innen) abzudecken. Auch hier sind einige Ausnahmen von der DSGVO normiert, allerdings nicht in dem Ausmaß wie zugunsten von Mediendiensten und –unternehmen.

Eine Zuständigkeit der DSB für die Behandlung von Beschwerden in diesem Kontext ist gegeben, wobei die **DSB einzelfallbezogen abzuwägen** hat, ob eine der in § 9 Abs. 1 und Abs. 1a DSG genannten Ausnahmen zur Anwendung gelangt. Dazu erging im Berichtszeitraum bereits eine Entscheidung, welche im Kapitel 4.2.1.1. näher dargestellt wird.

3.2.2. Die Einrichtung des Parlamentarischen Datenschutzkomitees

Mit Urteil vom 16. Jänner 2024 in der Rechtssache **C-33/22** entschied der EuGH aufgrund eines Vorabentscheidungsersuchens des VwGH, dass die DSGVO auch dann Anwendung findet, wenn – grob gesprochen – Daten durch Organe im Dienste der Gesetzgebung verarbeitet werden (dh. vor allem durch parlamentarische Organe; Anlass war ein Untersuchungsausschuss).

Des Weiteren entschied der EuGH, dass dann, wenn ein Mitgliedstaat nur eine Aufsichtsbehörde eingerichtet hat, diese eine umfassende, staatsgewaltenübergreifende Zuständigkeit hat. Damit wurde klargestellt, dass der DSB, als Organ der Staatsgewalt Verwaltung, eine Zuständigkeit gegenüber Organen der Staatsgewalt Gesetzgebung zukommt.

Als Folge dieses Urteils wurde mit der **Novelle BGBl. I Nr. 70/2024** in den **§§ 35a ff DSG** eine **eigene Datenschutz-Aufsichtsbehörde für alle Organe im Dienste der Bundesgesetzgebung, einschließlich der diesen zukommenden Verwaltungstätigkeiten**, eingerichtet: das **Parlamentarische Datenschutzkomitee (PDK)**.

Die DSB hat auch zu dieser Novelle eine umfassende Stellungnahme abgegeben (abrufbar unter https://www.parlament.gv.at/dokument/XXVII/SN/277391/imfname_1632404.pdf).

Der Aufsicht durch das PDK unterstehen **seit 1. Jänner 2025** nunmehr Datenverarbeitungen durch:

- den Nationalrat und den Bundesrat, einschließlich deren Mitglieder in Ausübung ihres Mandates sowie der Funktionäre gemäß § 56i Abs. 1 Z 1 bis 3 VfGG
- den Rechnungshof
- die Volksanwaltschaft
- die Parlamentsdirektion

Die bei der DSB zu diesem Zeitpunkt anhängigen Verfahren sind an das PDK abzutreten und von diesem fortzuführen. Zudem tritt das PDK bei Verfahren, die beim BVwG oder den Gerichtshöfen des öffentlichen Rechts anhängig sind, an die Stelle der DSB als belangte Behörde.

Organe im Dienste der Landesgesetzgebung können durch Landesverfassungsgesetz der Aufsicht durch das PDK unterstellt werden (sonst bleibt es bei einer Zuständigkeit der DSB).

Anders als die DSB ist das PDK eine Kollegialbehörde, bestehend aus mindestens drei, höchstens aber sechs Mitgliedern. Diese werden vom National- und vom Bundesrat mit Verfassungsmehrheit für eine Funktionsperiode von fünf Jahren gewählt, wobei Wiederwahlen zulässig sind. Sie üben ihre Tätigkeit nebenberuflich aus.

Das Vertretungsrecht im EDSA kommt dem Leiter der DSB zu.

Entscheidungen des PDK können, wie auch jene der DSB, vor dem BVwG angefochten werden, wobei im Falle des PDK – im Unterschied zur DSB – das BVwG durch einen Senat bestehend

aus drei Berufsrichtern entscheidet (bei Entscheidungen der DSB entscheidet ein 3-er Senat, bestehend aus einem Berufs- und zwei Laienrichtern, entsendet von der Wirtschafts- und der Arbeiterkammer).

Damit machte der Gesetzgeber von der Regelungsoption des Art. 51 Abs. 1 DSGVO Gebrauch, wonach in einem Mitgliedstaat auch mehr als eine Datenschutz-Aufsichtsbehörde eingerichtet werden kann.

Trotz des organisatorischen Naheverhältnisses zur Staatsgewalt Gesetzgebung handelt es sich beim PDK dennoch um eine Verwaltungsbehörde und nicht um ein Organ im Dienste der Gesetzgebung (siehe dazu auch die Ausführungen in VfGH 13.12.2023, G 212/2023 u.a., Rz 80).

3.3. Das Informationsfreiheitsgesetz – Rolle und Aufgaben der DSB

Das Informationsfreiheitsgesetz - IFG, BGBl. I Nr. 5/2024, tritt überwiegend mit **1. September 2025 in Kraft**. Nach **§ 4 Abs. 1 IFG** obliegt ab diesem Zeitpunkt informationspflichtigen Organen die **proaktive Informationspflicht**. Informationen von allgemeinem Interesse sind hierbei ehestmöglich in einer für jedermann zugänglichen Art und Weise im Internet zu veröffentlichen und bereit zu halten.

Zudem obliegt informationspflichtigen Organen und Einrichtungen nach **§ 7 IFG** ab diesem Zeitpunkt die **antragsgemäße Behandlung von Informationsbegehren**.

Nicht zur Veröffentlichung bestimmt und auf Antrag zugänglich zu machen, sind Informationen unter anderem nach **§ 6 Abs. 1 Z 7 lit. a IFG**, soweit und solange dies *„im überwiegenden berechtigten Interesse eines anderen, insbesondere […] zur Wahrung des Rechts auf Schutz der personenbezogenen Daten […] erforderlich und verhältnismäßig und gesetzlich nicht anders bestimmt ist. Zu diesem Zweck sind alle in Betracht kommenden Interessen, einerseits an der Erteilung der Information, darunter insbesondere auch an der Ausübung der Meinungsäußerungsfreiheit, und andererseits an der Geheimhaltung der Information, gegeneinander abzuwägen.“*

Gemäß **§ 15 Abs. 1 IFG** *„berät und unterstützt die [Datenschutzbehörde die] informationspflichtigen Organe bzw. Einrichtungen durch die Bereitstellung von Leitfäden und Angebote zur Fortbildung in datenschutzrechtlichen Belangen der Vollziehung der Informationsfreiheit.“*

Entsprechend den **Erläuterungen zu § 15 IFG (2238 dB XXVII. GP, 14)** soll die DSB demnach die informationspflichtigen Stellen im Hinblick auf die datenschutzrechtliche Rechtslage und Praxis (Rechtsprechung) beraten und unterstützen, indem sie allgemeine Anwendungshinweise und Anleitungen (Guidelines o.Ä.) zur Verfügung stellt und nach Möglichkeit regelmäßig geeignete Schulungsmaßnahmen anbietet.

Zudem hat die DSB gemäß **§ 15 Abs. 2 IFG** *„die Anwendung dieses Gesetzes begleitend zu evaluieren. Sie informiert die Öffentlichkeit über ihre Tätigkeit nach diesem Gesetz.“*

Damit ist klargestellt, dass die Aufgaben der DSB im Rahmen des IFG nicht der einer Informationsfreiheitsbehörde entsprechen.

Die DSB ist insbesondere nicht dazu berufen, Streitigkeiten zwischen Antragsteller:innen und auf der einen und informationspflichtigen Stellen auf der anderen Seite zu schlichten.

Ihre **Rolle als Aufsichtsbehörde nach der DSGVO bleibt** davon **unberührt.**

Um die ihr übertragenen Aufgaben bestmöglich wahrnehmen zu können, hat die DSB im Jahr 2024 folgende Schritte gesetzt:

- Am 6. Mai 2024 hat die DSB ein erstes Rundschreiben an die informationspflichtigen Organen bzw. Einrichtungen mit fünf Fragestellungen übermittelt. Dies vor dem Hintergrund, dass der Leitfaden sowie die Schulungsmaßnahmen möglichst effektiv gestaltet werden können.
- Bis zum 30. Juni 2024 langten ca. 80 Stellungnahmen ein, die anschließend gesichtet wurden.
- Am 24. September 2024 fand im Festsaal des Bundesministeriums für Justiz die erste Informationsveranstaltung statt. Über 100 Teilnehmer:innen aus ganz Österreich aus allen Bereich der Verwaltung, sowohl auf Bundes- als auch Landesebene, Universitäten und Kammern waren anwesend. Die Tagesordnung umfasste unter anderem einen Vortrag von Herrn Reto Ammann, Leiter des Direktionsbereichs Öffentlichkeitsprinzip beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).
- Nach diesem Informationsaustausch erarbeitete die DSB bis zum Jahresende den ersten Entwurf eines Leitfadens für informationspflichtige Organe bzw. Einrichtungen.
- Am 13. Jänner 2025 wurde dieser Entwurf zur Begutachtung versendet. Der Leitfaden kann über die Website der DSB eingesehen werden (https://dsb.gv.at/informationsfreiheitsgesetz/informationsfreiheitsgesetz).
- Im Laufe des ersten Halbjahres 2025 werden die gesetzlich angeordneten Schulungsmaßnahmen durch die DSB durchgeführt.

Die DSB hält fest, dass ihr für die Umsetzung dieser Maßnahmen keine zusätzlichen Planstellen zur Verfügung gestellt wurden. Jedoch hatte sie die Möglichkeit, 5 Verwaltungspraktikanti:nnen zu beschäftigen, sodass es nur zu geringfügigen Einschränkungen bei den von ihr wahrzunehmenden Aufgaben kam.

3.4. Die europäische Verordnung über Künstliche Intelligenz (KI-VO) – erste Ableitungen für die Tätigkeit der DSB

Als Künstliche Intelligenz werden verschiedene Technologien bezeichnet, die im gesamten Spektrum von Wirtschaft und Gesellschaft zunehmend zum Einsatz kommen. Zur Regulierung dieser Technologien wurde die **Verordnung (EU) 2024/1689 über Künstliche Intelligenz** (KI-VO)[2] **am 21. Mai 2024 formal angenommen**. Dieses Regelwerk der EU wird in den nächsten Monaten und Jahren schrittweise anwendbar sein. Die Vorgaben gemäß **Art. 5 KI-VO für verbotene Praktiken** im KI-Bereich gelten bereits **seit 2. Februar 2025**, die **zuständigen nationalen Behörden** sind **bis 2. August 2025 zu benennen**.

2 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401689

Nach **Art. 2 Abs. 7 KI-VO** bleibt die DSGVO von der KI-VO unberührt. Daraus folgt, dass die **KI-VO sowie die DSGVO parallel anwendbar** sind und eine Zuständigkeit der DSB gegeben ist, sofern personenbezogene Daten im Rahmen von KI-Systemen verarbeitet werden.

Die DSB hat dies zum Anlass genommen, die datenschutzrechtlichen Implikationen der KI-VO zu prüfen. Im Berichtszeitraum wurden entsprechende Informationen auf der **Website der DSB** veröffentlicht (**FAQ betreffend KI und Datenschutz**) und ein **Rundschreiben an Verantwortliche des öffentlichen und privaten Bereichs** verschickt, um auf dieses Thema aufmerksam zu machen.[3]

Auf internationaler Ebene brachte sich die DSB in den einschlägigen Fachgruppen des EDSA ein und wirkte zuletzt bei der **Stellungnahme 28/2024 hinsichtlich datenschutzrechtlicher Fragestellungen im Kontext von KI-Modellen** mit.[4] Die Ausarbeitung detaillierter Leitlinien zum Thema Datenschutz und KI ist wichtiger Bestandteil der Strategie des EDSA für die kommenden Jahre.

Abseits der Kompetenzen, die sich bereits aus der DSGVO ergeben, können der DSB aufgrund der KI-VO weitere Aufgaben übertragen werden. Zum aktuellen Zeitpunkt steht die Benennung der Behörden gemäß **Art. 70 KI-VO** auf nationaler Ebene noch aus. Eine unmittelbare Zuständigkeit sieht **Art. 74 Abs. 8 KI-VO** vor, wonach der DSB (nach derzeitiger Rechtslage) die Aufgabe als **Marktüberwachungsbehörde für gewisse Hochrisiko-KI-Systeme** u.a. in den Bereichen Strafverfolgungszwecke und Grenzmanagement zukommt. Damit verbunden ist eine punktuelle Zuständigkeit als notifizierte Stelle gemäß **Art. 43 Abs. 1 zweiter UAbs. KI-VO**.

Darüber hinaus legt **Art. 77 KI-VO** fest, dass für den Schutz der Grundrechte zuständige Behörden im Rahmen ihrer Aufgaben u.a. Dokumentationen anfordern können, die nach der KI-VO zu führen sind. Zudem kann bei der entsprechenden Marktüberwachungsbehörde ein Antrag auf Durchführung eines technischen Tests von Hochrisiko-KI-Systemen gestellt werden. Die DSB wurde der Europäischen Kommission bereits als Grundrechtsbehörde gemäß Art. 77 KI-VO notifiziert.

Zur Vorbereitung auf diese neuen Aufgaben wird die DSB auch im Jahr 2025 in einen **intensiven Austausch mit anderen Behörden auf nationaler und internationaler Ebene** treten. Gleichzeitig wird das Informationsangebot zum Thema KI und Datenschutz weiter ausgebaut. Über diesbezügliche Entwicklungen informiert die DSB laufend auf ihrer Webseite.

3.5. Weitere Rechtsakte der EU mit unmittelbaren Auswirkungen auf die Tätigkeit der DSB

Neben der bereits erwähnten KI-VO werden zeitnah weitere EU-Rechtsakte (teilweise) in Geltung treten, die Auswirkungen auf das Datenschutzrecht und somit auch auf die Tätigkeit der DSB haben.

Diese werden in Folge überblicksmäßig dargestellt:

3 https://dsb.gv.at/kuenstlichebrintelligenz/kuenstliche-intelligenz-datenschutz
4 https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

Von besonderer Bedeutung ist die **VO (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung(Targeting-VO)**[5], die (vollumfänglich) **ab** dem **10. Oktober 2025** gilt. Die Verordnung legt harmonisierte Vorschriften für ein hohes Maß an Transparenz in Bezug auf politische Werbung (und damit verbundene Dienstleistungen) fest. In diesem Zusammenhang wird auch die Verarbeitung personenbezogener Daten behandelt.

Konkret sehen etwa die **Art. 18, 19 Targeting-VO spezielle Pflichten für das Targeting und die Anzeigenschaltung im Zusammenhang mit politischer Werbung im Internet** vor. Hervorzuheben ist etwa, dass derartige Anzeigeschaltungen (und die damit verbundene Datenverarbeitung) nicht auf Profiling beruhen dürfen. Für die Datenverarbeitung zum Zwecke politischer Werbung im Zuge von Targeting- und Anzeigenschaltungsverfahren müssen zudem näher bestimmte Voraussetzungen berücksichtigt werden (z.B. müssen die Daten von der betroffenen Person mit ihrer ausdrücklichen Einwilligung für Zwecke der politischen Werbung erhoben werden).

Die **Überwachung der Anwendung** dieser Bestimmungen **obliegt nach Art. 22 Abs. 1 Targeting-VO der DSB** in ihrem Zuständigkeitsbereich. Zu diesem Zweck gelten die Befugnisse der DSB gemäß **Art. 58 DSGVO** sinngemäß (insbesondere die Untersuchungs- und Abhilfebefugnisse). Ausdrücklich normiert wird, dass bei Verstößen gegen die genannten Bestimmungen die DSB innerhalb ihrer Zuständigkeit Geldbußen im Einklang mit **Art. 83 DSGVO** bis zu einem Betrag von EUR 20.000.000,- oder 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher Betrag höher ist, verhängen kann (**Art. 25 Abs. 6 Targeting-VO**). Dadurch wir die Strafkompetenz der DSB erweitert.

Zusammen mit den anderen Aufsichtsbehörden muss die DSB im Rahmen des EDSA zudem **Leitlinien über die Anforderungen dieser Verordnung** ausarbeiten (**Art. 22 Abs. 2 Targeting-VO**).

Die **RL 2022/2555 (NIS-2-RL)** ersetzt die alte NIS-RL und sieht Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU vor. Auf nationaler Ebene steht die Umsetzung der NIS-2-RL noch aus, ein entsprechender Entwurf (Informationssystemsicherheitsgesetz) scheiterte an der erforderlichen Zweidrittelmehrheit im Nationalrat.[6] Dieser Rechtsakt verweist punktuell auf die DSGVO und sieht insbesondere bei Sicherheitsvorfällen („Data Breaches“) eine **enge Zusammenarbeit zwischen der DSB und den zuständigen Behörden nach der NIS-2-RL** vor. Die Zusammenarbeit mit der DSB wird dabei in **§ 21 des Entwurfes** behandelt.

Eine enge Zusammenarbeit mit der künftigen „**Cybersicherheitsbehörde**“ ist darüber hinaus auch für die Verhängung von Geldbußen erforderlich, um eine allfällige Doppelbestrafung in Bezug auf dasselbe Verhalten zu vermeiden. Im Entwurf werden im 5. Hauptstück die Strafbestimmungen (**§ 45**) sowie die Zuständigkeit und allgemeine Bedingungen für die Verhängung von Geldbußen (**§ 44**) geregelt.

Die Verhängung von Geldbußen obliegt laut Entwurf den Bezirksverwaltungsbehörden und diese sind wiederum verpflichtet, die Cybersicherheitsbehörde über die Einleitung von allfälligen Verwaltungsstrafverfahren zu informieren. In diesem Zusammenhang wird ausdrücklich vorgesehen, dass die Bezirksverwaltungsbehörden keine Geldstrafe verhängen dürfen, wenn

5 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32024R0900
6 https://www.parlament.gv.at/gegenstand/XXVII/A/4129

der in Verdacht stehende Verstoß durch dasselbe Verhalten bereits Gegenstand einer Geldbuße der DSB nach Art. 83 DSGVO war (**§§ 21 Abs. 3 und 44 Abs. 7**).

Die **VO 2022/2065 über einen Binnenmarkt für digitale Dienste (DSA**) regelt die Pflichten und Verantwortlichkeiten von Online-Plattformen und digitalen Diensten innerhalb der EU.[7] Diese Verordnung gilt bereits seit dem **17. Februar 2024**. Auf nationaler Ebene ist die **KommAustria** gemäß **§ 2 Abs. 1 KDD-G** als zuständige Behörde vorgesehen (unterstützt durch die RTR-GmbH, Fachbereich Medien). Soweit datenschutzrechtliche Fragen im Zusammenhang mit dem Digital Services Act betroffen sind, ist die DSB im engen Austausch mit der KommAustria.

Seit **17. Jänner 2025** sind die Vorgaben der **VO 2022/2554 über die digitale operationale Resilienz im Finanzsektor** (**DORA**) zu beachten.[8] DORA legt Anforderungen an das Risikomanagement, die Meldung von Zwischenfällen, die Prüfung der Informations- und Kommunikationstechnologie (IKT) sowie die Abhängigkeiten von Drittanbietern fest. Soweit personenbezogene Daten von einem Sicherheitsvorfall betroffen sind, besteht wiederum die Notwendigkeit der **Zusammenarbeit zwischen der DSB und der gemäß DORA kompetenten Behörde (FMA**).

Die **VO 2023/2854 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung** (**Daten-VO**, besser bekannt als **Data Act**) tritt ab dem **12. September 2025** (vollumfänglich) in Geltung.[9] Zusammengefasst soll die Nutzung von Daten durch Regeln für deren Austausch und Verfügbarkeit gefördert werden. Soweit im Rahmen des Datenzugangs personenbezogene Daten betroffen sind, kommt der DSB gemäß **Art. 37 Abs. 3 Daten-VO** eine entsprechende Zuständigkeit zu.

Schließlich ist die **VO 2022/868 über europäische Daten-Governance, der sogenannte Data Governance Act (DGA)** zu erwähnen, deren Zielsetzung insbesondere die Förderung der Weiterverwendung von Daten des öffentlichen Sektors ist.[10] Ein Entwurf für ein nationales Begleitgesetz (**Datenzugangsgesetz**) liegt bereits vor.[11]

3.6. Neue Webseite der DSB

Der Internetauftritt der DSB **www.dsb.gv.at** wurde im Jahr 2024 grundlegend überarbeitet und unter „Aktuelles“ wird die DSB vermehrt über ihre Arbeit und die wichtigsten datenschutzrechtlichen Entwicklungen informieren.

Neben einem gänzlich neuen, optisch ansprechenderen Layout wurde insbesondere an einer besseren Übersicht über die datenschutzrechtlich relevantesten Themen, wie etwa Videoüberwachung und künstliche Intelligenz, sowie an einer schlüssigeren Gliederung der Seiteninhalte gearbeitet.

Darüber hinaus bietet die Datenschutzbehörde auf der neuen Website neben den bestehenden Online-Formularen zur Einbringung von Beschwerden bzw. zur Anregung von amtswegigen

7 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02022R2065-20221027
8 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2554.
9 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202302854
10 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02022R0868-20220603
11 https://www.parlament.gv.at/gegenstand/XXVII/ME/352?selectedStage=100

Prüfverfahren auch ein **neues Online-Formular zur vereinfachten Meldung von Verletzungen des Schutzes personenbezogener Daten** an („**Data Breach-Meldung**“).

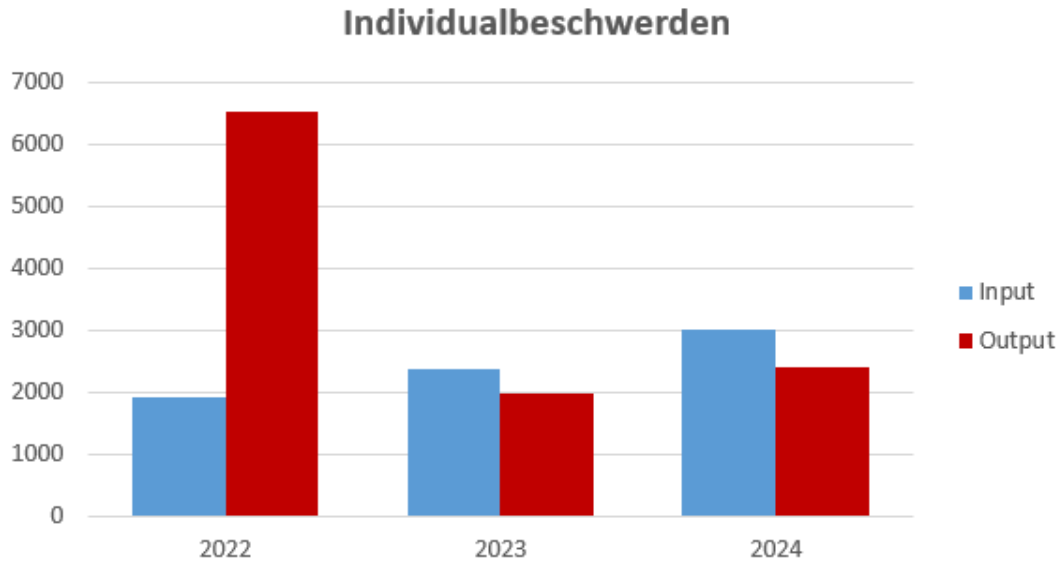
4. Tätigkeit der Datenschutzbehörde

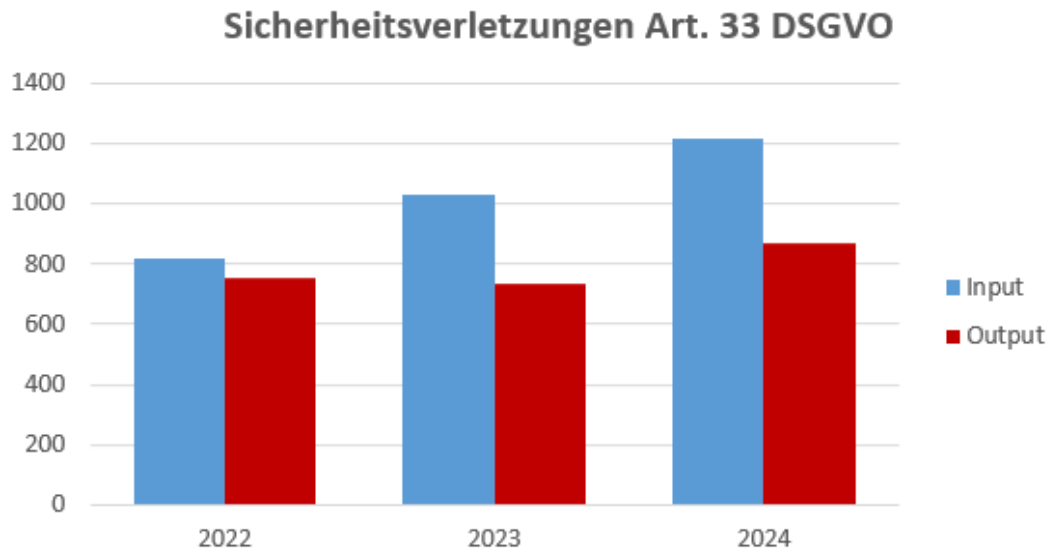
4.1 Statistische Darstellung

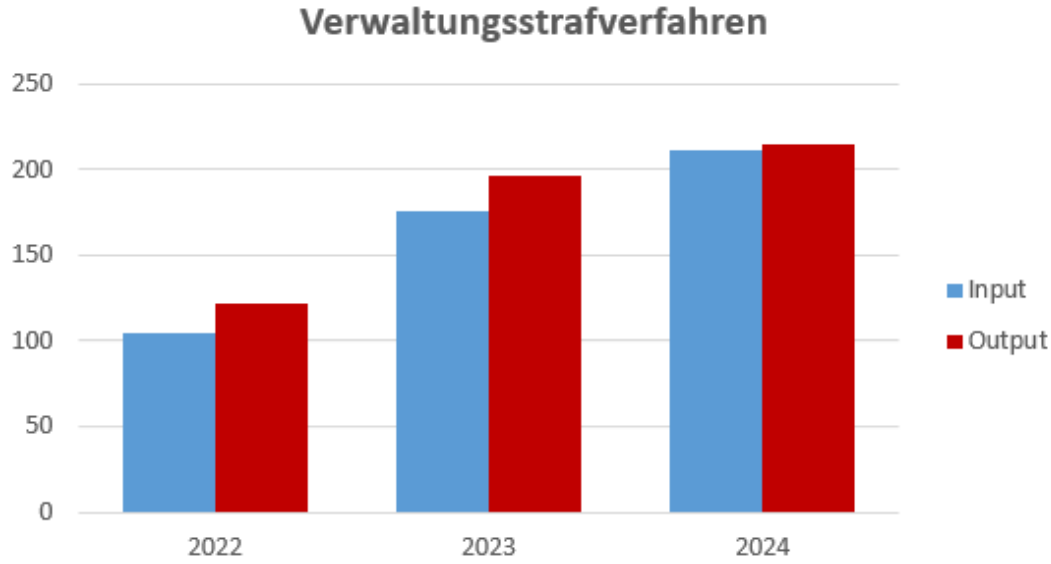
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2022	2023	**2024**	2022	2023	**2024**
BESCHWERDEN - Inland						
Individualbeschwerden	1915	2389	**3019**	6517	1978	**2397**
Erledigungsart der Individualbeschwerden				4806 Bescheide 1712 Einstellungen	1485 Bescheide 493 Einstellungen	1845 Bescheide 552 Einstellungen
BESCHWERDEN - Ausland						
Beschwerden grenzüberschreitend (im Ausland einlangend)	374	443	**194**	130	76	**27**
- davon: Beschwerden grenzüberschreitend (im Ausland einlangend, One Stop Shop - Österreich betroffen) ***IMI:*** *Internal Market Information System*			175 (von insgesamt 856 über IMI eingelangten Meldungen)			17 Einstellungen
- davon: Beschwerden grenzüberschreitend (im Ausland einlangend, O.S.S. - Österreich federführend)			19			3 Bescheide 7 Einstellungen
Beschwerden grenzüberschreitend (in Österreich einlangend)	236	433	**600**	171	364	**275**
- davon: Beschwerden grenzüberschreitend (in Österreich einlangend - Behandlung im O.S.S)			511			96 Bescheide 147 Einstellungen
- davon: Beschwerden grenzüberschreitend (in Österreich einlangend – Drittstaat, keine O.S.S. - Behandlung in Österreich)			89			9 Bescheide 23 Einstellungen

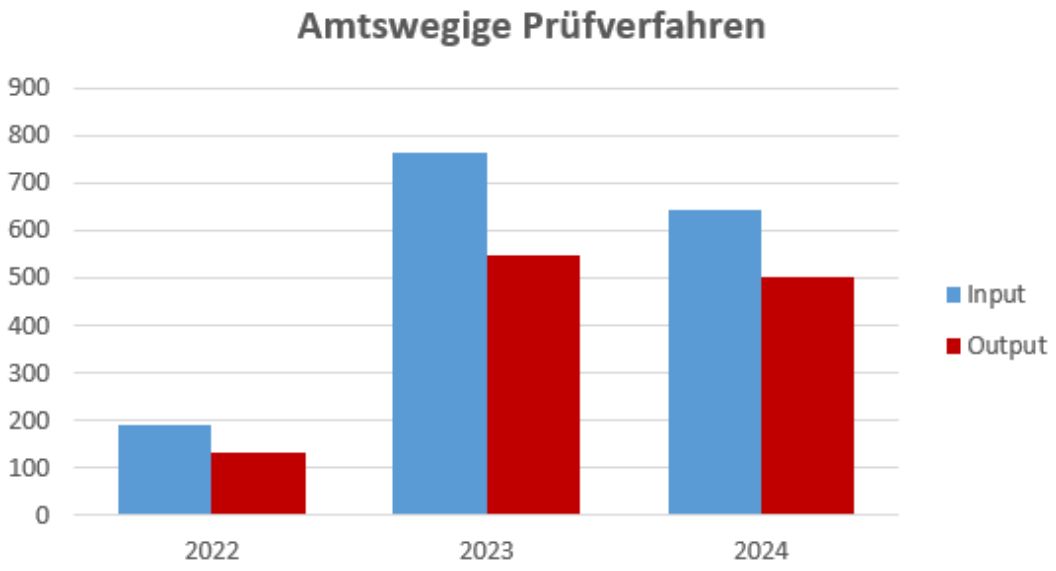
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2022	2023	**2024**	2022	2023	**2024**
AMTSWEGIGE PRÜFVERFAHREN						
Amtswegige Prüfverfahren	190	765	**646**	133	549	**504**
Erledigungsart der amtswegigen Prüfverfahren				11 Bescheide 122 Einstellungen	12 Bescheide 537 Einstellungen	8 Bescheide 496 Einstellungen
VERWALTUNGSSTRAFVERFAHREN						
Verwaltungsstrafverfahren	105	176	**211**	122	196	**214**
Erledigungsart der Verwaltungsstrafverfahren				63 Bescheide 59 Einstellungen	58 Bescheide 138 Einstellungen	62 Bescheide 152 Einstellungen
SICHERHEITSVERLETZUNGEN						
Sicherheitsverletzungen nach dem TKG	25	28	**55**	25	19	**36**
Sicherheitsverletzungen Art. 33	818	1028	**1216**	751	734	**870**
Sicherheitsverletzungen grenzüberschreitend (in Österreich einlangend)	15	30	**39**	9	20	**27**
Sicherheitsverletzungen grenzüberschreitend (im Ausland einlangend)	20	26	**9**	3	13	**3**
VERFAHREN VOR DEM BUNDESVERWALTUNGSGERICHT						
Verfahren vor dem BVwG -gesamt	1193	613	**301**			
- davon Bescheidbeschwerden	1156	579	**245**			
- davon Säumnisbeschwerden	37	34	**56**			

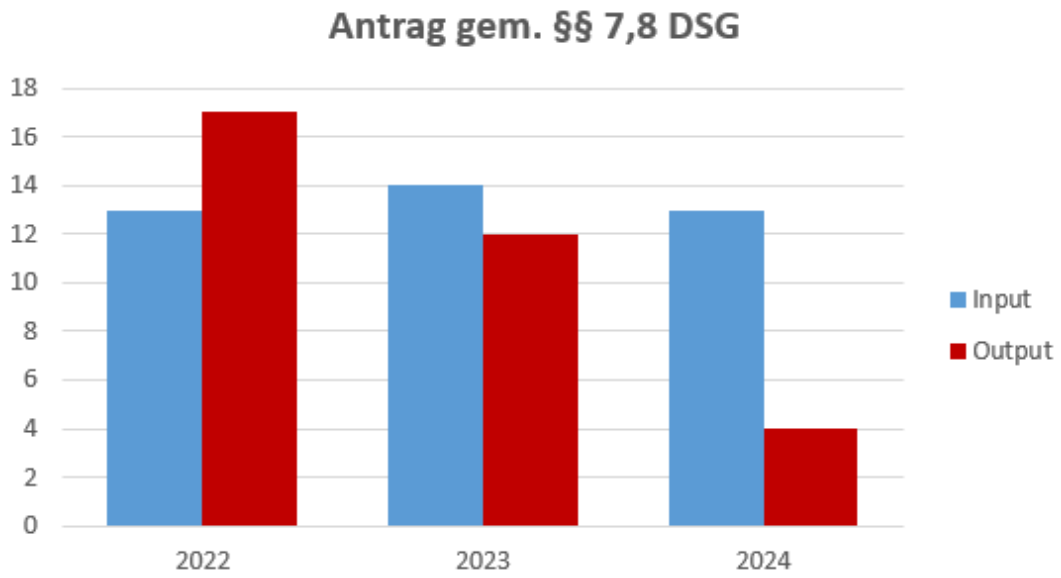
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2022	2023	**2024**	2022	2023	**2024**
RECHTSAUSKÜNFTE/ANFRAGEN						
Schriftliche Rechtsauskünfte	3069	1842	**1935**	3069	1842	**1935**
Telefonische Rechtsauskünfte			**224**			**224**
Telefonische Anfragen, welche im Rahmen der Kanzleitätigkeit erledigt wurden			**ca. 5500**			**ca. 5500**
Schriftverkehr mit Behörden	239	185	**265**	239	185	**265**
Schriftverkehr mit privaten Einrichtungen			**105**			**105**
Allgemeine Anfragen aus dem Ausland	52	68	**56**			
Amtshilfeersuchen international über IMI einlangend (Art. 61 DSGVO)		624	**612**			
Amtshilfeersuchen international ausgehend (Art. 61 DSGVO)		242	**199**			
SONSTIGES						
Anträge auf Genehmigung nach §§ 7 und 8 DSG (wissenschaftliche Forschung u. Statistik)	13	14	**13**	17	12	**4**
Konsultationsverfahren	3	1	**1**	3	2	**2**
Anträge auf Genehmigung im internationalen Datenverkehr	1	0	**0**	1	0	**0**
Anträge auf Genehmigung von Verhaltensregeln	2	0	**1**	5	0	**1**
Co-Reviews (Art. 64 Abs. 1 DSGVO)			**4**			**4**
Genehmigung BCR (International)	0	0	**0**	2	0	**0**
Zertifizierungskriterien (Art. 42 DSGVO)	2	2	**1**	1	1	**2**
Akkreditierte Zertifizierungsstellen			**1**			**1**
Meldungen von Datenschutzbeauftragten	602	642	**610**	602	642	**610**
Auskunft aus dem Schengen Information System (SIS)	746	336	**285**	746	336	**285**
Geltendmachung von Betroffenenrechten gegenüber der DSB			**50**			**50**

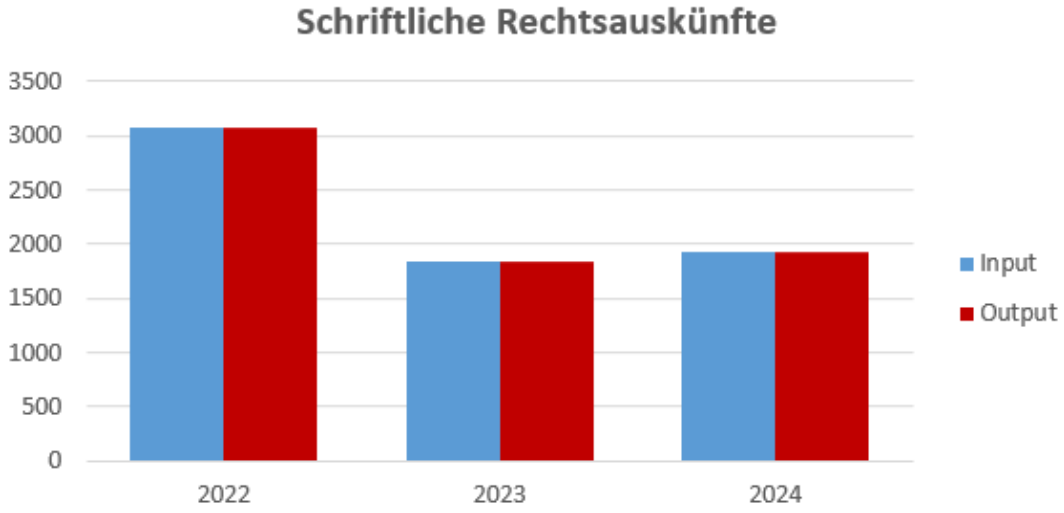

Individualbeschwerden
7000
6000
5000
4000
3000
2000
1000
0
2022
2023
2024
Input
Output

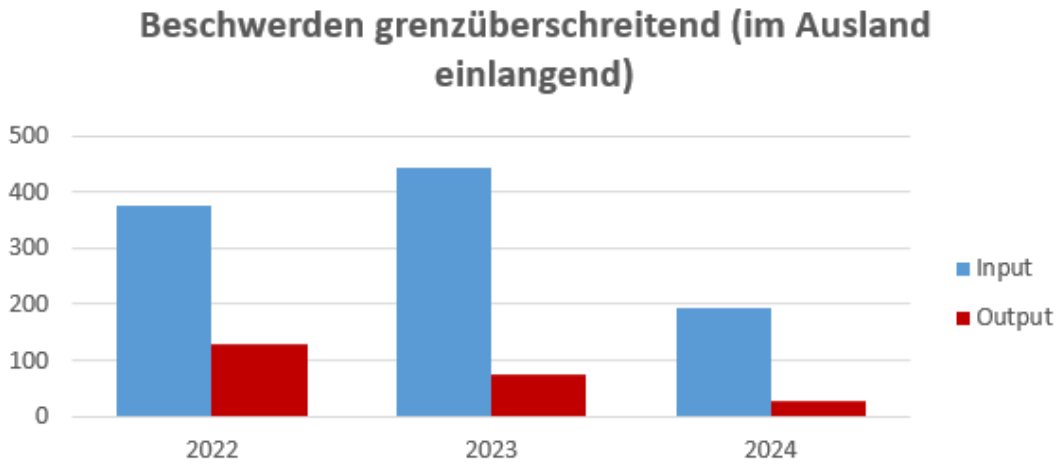

Sicherheitsverletzungen Art. 33 DSGVO
1400
1200
1000
800
600
400
200
0
2022
2023
2024
Input
Output

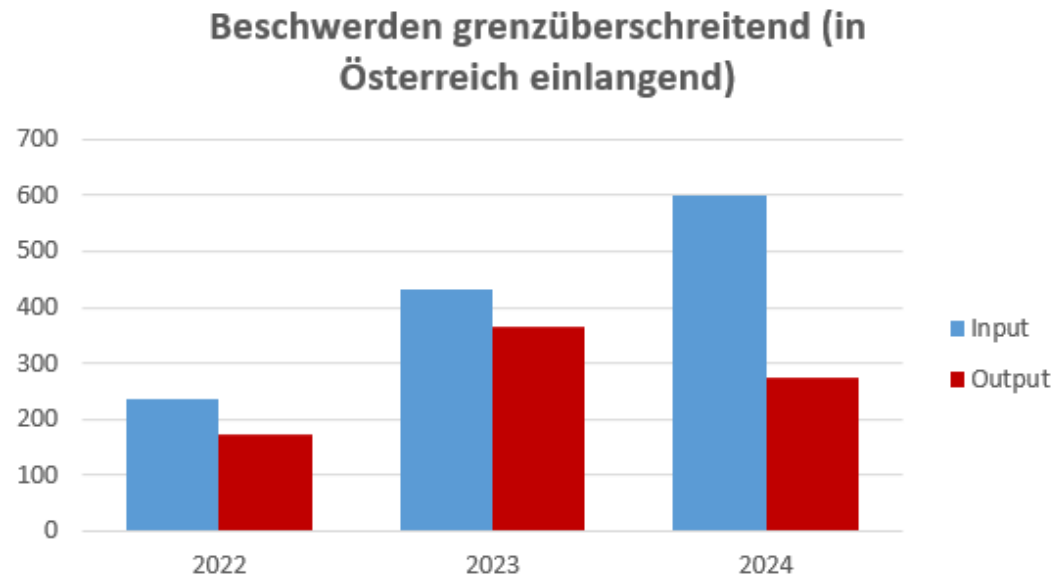

Verwaltungsstrafverfahren
250
200
150
100
50
0
2022
2023
2024
Input
Output


Amtswegige Prüfverfahren
900
800
700
600
500
400
300
200
100
0
2022
2023
2024
Input
Output


Antrag gem. §§ 7,8 DSG
18
16
14
12
10
8
6
4
2
0
2022
2023
2024
Input
Output


Schriftliche Rechtsauskünfte
3500
3000
2500
2000
1500
1000
500
0
2022
2023
2024
Input
Output





4.2 Verfahren und Auskünfte

4.2.1.1 Individualbeschwerden

1. Bescheid vom 4. Jänner 2024, GZ: D124.889 (OZ: 2023-0.915.031)
Verarbeitung bonitätsrelevanter Informationen über Schuldenregulierungsverfahren durch eine Wirtschafts- und Kreditauskunftei über den Zeitraum ihrer Veröffentlichung in der Insolvenzdatei

Den Kern dieses Verfahrens bildete die Frage, ob und wie lange Gewerbetreibende iSd. § 152 GewO („Auskunfteien über Kreditverhältnisse“) bonitätsrelevante Informationen über Schuldenregulierungsverfahren, welche sie aus öffentlichen Registern erhoben haben, in ihren privaten Bonitätsdatenbanken zwecks Erteilung von Auskünften über die Kreditwürdigkeit der betroffenen Personen verarbeiten dürfen. Der EuGH hat in diesem Zusammenhang mit Urteil vom 7. Dezember 2023 in den verbundenen Rechtssachen C-26/22 und C-64/22 entschieden,

dass eine Speicherung von aus öffentlichen Registern stammenden Informationen über Insolvenzen natürlicher Personen durch private Wirtschaftsauskunfteien für einen Zeitraum, der über die Speicherdauer dieser Daten in den öffentlichen Registern hinausgeht, nicht mit den in der DSGVO verankerten Grundsätzen der Verarbeitung und Rechtmäßigkeit im Einklang steht. Im von der DSB zu prüfenden Sachverhalt wurden aus der Insolvenzdatei erhobene Informationen über ein im Jahr 2016 abgeschlossenes Sanierungsverfahren von einer Wirtschafts- und Kreditauskunftei bis ins Jahr 2023 verarbeitet. Gestützt auf die zuvor zitierte Rechtsprechung des EuGH stellte die DSB eine Rechtsverletzung fest, da die verfahrensgegenständlichen Informationen über den Zeitraum ihrer öffentlichen Abrufbarkeit iSd. § 256 IO verarbeitet worden sind.

Dieser Bescheid ist rechtskräftig.

2. Bescheid vom 16. Mai 2024, GZ: DSB-D124.0495/22 (OZ: 2023-0.607.511)
Fehlende Aufzeichnungen über Herkunft und Empfänger der Daten sowie unterlassene Information nach Art. 14 DSGVO durch ein das Gewerbe nach § 151 GewO ausübendes Unternehmen (Adressverlage und Direktmarketingunternehmen)

Die Beschwerdegegnerin, die das Gewerbe der Adressverlage und Direktmarketingunternehmen nach § 151 GewO ausübt, verarbeitet personenbezogene Daten des Beschwerdeführers, mit dem sie jedoch in keinem Vertragsverhältnis steht. Der Beschwerdeführer wurde von der Beschwerdegegnerin über die Datenverarbeitung nicht informiert. Im Zuge einer datenschutzrechtlichen Auskunft gab sie an, dass sie über keine Informationen zur Herkunft der verarbeiteten Daten sowie zu den Datenempfängern verfüge.

Die Beschwerdegegnerin rechtfertigte die fehlende Information einerseits mit dem Ausnahmetatbestand des Art. 14 Abs. 5 lit. b DSGVO, wonach die Informationserteilung einen unverhältnismäßig hohen Aufwand verursachen würde und andererseits mit dem Ausnahmetatbestand des Art. 14 Abs. 5 lit. c DSGVO und führte dazu die Bestimmung des § 151 GewO als Rechtsgrundlage an.

Die DSB gab der Beschwerde statt und stellte fest, dass die Beschwerdegegnerin Art. 5 Abs. 1 lit. a und d DSGVO iVm Art. 24 DSGVO und Art. 25 DSGVO verletzt hat, indem sie die Einhaltung der in den genannten Bestimmungen festgelegten Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten des Beschwerdeführers gemäß Art. 5 Abs. 2 DSGVO nicht nachweisen konnte.

Eine Verletzung von Art. 5 Abs. 1 lit. a DSGVO (Grundsatz der Transparenz) liegt vor, weil die Beschwerdegegnerin nicht nachweisen konnte, dass sie die Bestimmung in Bezug auf die Verarbeitung der personenbezogenen Daten des Beschwerdeführers eingehalten hat. Etwa erscheint das bloße Abstellen auf eine hohe Anzahl an Datensätzen nicht ausreichend, um den nach Art. 14 Abs. 5 lit. b DSGVO geforderten unverhältnismäßigen Aufwand zu begründen, andererseits hat die Beschwerdegegnerin auch nicht dargelegt, dass sie geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen hat.

Eine Verletzung von Art. 5 Abs. 1 lit. d DSGVO (Grundsatz der Richtigkeit) wurde deshalb festgestellt, weil die Beschwerdegegnerin ehemalige postalische Anschriften des Beschwerdeführers verarbeitet. Besonders im Hinblick auf ein das Gewerbe nach § 151 GewO ausübendes Unternehmen sollte jedoch besonderes Augenmerk daraufgelegt werden, dass aktuelle Adressen

verarbeitet werden, zumal aufgrund fehlender Aufzeichnung der Datenempfänger auch nicht ausgeschlossen werden kann, dass die historischen Adressen an Dritte übermittelt werden.

Eine Verletzung von Art. 24 und 25 DSGVO führt nicht zur Unrechtmäßigkeit der Datenverarbeitung. Da die Beschwerdegegnerin es jedoch unterlassen hat, ein Vorbringen zu technischen und organisatorischen Maßnahmen in Bezug auf die Verarbeitung der personenbezogenen Daten des Beschwerdeführers zu erstatten, ist sie auch diesbezüglich ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO iVm Art. 5 Abs. 1 lit. a und lit. d DSGVO nicht nachgekommen.

Dieser Bescheid ist rechtskräftig.

3. Bescheid vom 4. Juli 2024, GZ: DSB-D124.2340/23 (OZ: 2024-0.199.724)
Die Veröffentlichung von Parteispenden durch den österreichischen Rechnungshof ist rechtmäßig aufgrund einer gesetzlicher Grundlage gemäß § 6 Abs. 2 und Abs. 3 PartG

Die Parteispende des Beschwerdeführers, welche über 2.500 Euro betrug, wurde auf der Webseite des Rechnungshofs mit den Informationen Partei, Datum, Name des Spenders, PLZ des Spenders und Betrag veröffentlicht. Der Beschwerdeführer erhob dagegen Beschwerde wegen einer behaupteten Verletzung im Recht auf Geheimhaltung iSd. § 1 Abs. 1 DSG und brachte insbesondere vor, dass § 6 Abs. 2 und Abs. 3 PartG in seiner Reichweite unverhältnismäßig sei und nicht von angemessenen und spezifischen Maßnahmen zu Wahrung der Grundrechte und Interessen der betroffenen Personen flankiert sei. Es käme somit keine Ausnahme von dem Verbot des Art. 9 Abs. 2 DSGVO zum Tragen.

Die DSB stellte fest, dass es sich gegenständlich um sensible Daten iSd. Art. 9 DSGVO handelte, da die politische Meinung des Beschwerdeführers aus der gegenständlichen Veröffentlichung seiner Parteispende hervorgeht.

Jedoch bildet § 6 Abs. 2 und Abs. 3 PartG jedenfalls eine gesetzliche Grundlage iSd. Art. 9 Abs. 2 lit. g DSGVO. Auch das von Art. 9 Abs. 2 lit. g DSVGO geforderte „erhebliche öffentliche Interesse“ ist nach Auffassung der DSB gegeben, da die Transparenz der Parteienfinanzierung jedenfalls ein solches erhebliches öffentliches Interesse darstellt.

Die gegenständliche Datenverarbeitung ist insbesondere auch deswegen verhältnismäßig, da nun nicht mehr – wie noch in der Fassung des § 6 Abs. 4 PartG in BGBl. I Nr. 55/2019 vorgesehen - die gesamte Anschrift des Beschwerdeführers veröffentlicht wird (sondern nur die Postleitzahl). Darüber hinaus wurden durch Festlegung einer Löschfrist (§ 6 Abs. 2 letzter Satz PartG) sowie im Rahmen der durchgeführten Datenschutz-Folgenabschätzung und in Form von einer festgelegten Kaskade (erhöhte Eingriffsintensität bei höherer finanzieller Zuwendung an die Partei) angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen iSd. Art. 9 Abs. 2 lit. g DSGVO umgesetzt.

Der Bescheid ist nicht rechtskräftig.

Aufgrund des Urteils des EuGH vom 16. Jänner 2024 zu C-33/22 war die DSB für das gegenständliche Verfahren gegen ein Organ der Gesetzgebung (Rechnungshof) noch zuständig.

Die Zuständigkeit als belangte Behörde im Verfahren vor dem BVwG ging jedoch ab 1. Jänner 2025 auf das neu eingerichtete „Parlamentarische Datenschutzkomitee“ über (siehe BGBl. I Nr. 70/2024).

4. Teilbescheid vom 9. August 2024, GZ: D130.1949 (OZ: 2024-0.421.248)
Kein subjektives Recht auf Erlassung einstweiliger Maßnahmen im Rahmen des Dringlichkeitsverfahrens nach Art. 66 DSGVO

Gegenstand dieses Beschwerdeverfahrens waren behauptete Rechtsverletzungen im Rahmen der Verwendung personenbezogener Daten durch ein im EWR niedergelassenes Unternehmen für Technologien der künstlichen Intelligenz. In diesem Zusammenhang wurde in der Beschwerde ausdrücklich auch die Verhängung einstweiliger Maßnahmen in Form eines vorläufigen Verbots der Verarbeitung im Rahmen eines Dringlichkeitsverfahrens gemäß Art. 66 DSGVO beantragt. Gemäß dieser Bestimmung kann jede betroffene Aufsichtsbehörde in Abweichung vom Verfahren nach Art. 56 ff DSGVO in ihrem Hoheitsgebiet zeitlich befristete Maßnahmen zum Schutz der Rechte und Freiheiten von betroffenen Personen erlassen.

Mit Teilbescheid vom 9. August 2024 wies die DSB den Antrag auf Verhängung einstweiliger Maßnahmen zurück. Begründend wurde ausgeführt, dass in Hinblick auf Art. 66 Abs. 1 DSGVO zwar nicht bestritten werden kann, dass diese Bestimmung im Ergebnis darauf ausgerichtet ist, Rechte und Freiheiten von betroffenen Personen zu schützen, sie aber ausdrücklich als „Kann"-Bestimmung formuliert ist. Gleichsam ist die Einholung von Stellungnahmen des EDSA betreffend die Erlassung von endgültigen Maßnahmen gemäß Abs. 2 leg. cit. oder betreffend die Untätigkeitsrüge gegen eine andere Aufsichtsbehörde gemäß Abs. 3 leg. cit. als „Kann"-Bestimmungen normiert und es kann hieraus keine Verpflichtung einer Datenschutzaufsichtsbehörde zur Ergreifung solcher Schritte abgeleitet werden.

Das Dringlichkeitsverfahren gemäß Art. 66 DSGVO stellt zudem – im Unterschied zum Stellungnahmeverfahren gemäß Art. 64 DSGVO und dem Streitbeilegungsverfahren gemäß Art. 65 DSGVO – keinen eigenständigen Verfahrenstypus, sondern eine punktuell modifizierte und beschleunigte Variante des Stellungnahme- bzw. Streitbeilegungsverfahrens dar, in dem der EDSA verbindlich über Meinungsdivergenzen und Konflikte zwischen Aufsichtsbehörden (und nicht zwischen Betroffenen und Datenschutzaufsichtsbehörden) entscheidet.

Ferner war zu beachten, dass sich vorläufige (und auch endgültige) Maßnahmen gemäß Art. 66 DSGVO denkmöglich nur in Form von Abhilfebefugnissen iSd. Art. 58 Abs. 2 DSGVO manifestieren können und der EuGH in diesem Zusammenhang bereits mehrfach ausgesprochen hat, dass es im Ermessen der Aufsichtsbehörde liegt, von geeigneten Abhilfebefugnissen Gebrauch zu machen, um über die umfassende Einhaltung der DSGVO zu wachen. Ein subjektiver Rechtsanspruch auf Erlassung einstweiliger Maßnahmen im Rahmen eines Dringlichkeitsverfahrens nach Art. 66 DSGVO besteht vor diesem Hintergrund nicht.

Der Teilbescheid ist rechtskräftig.

5. Bescheid vom 28. Oktober 2024, GZ: DSB-D124.0507/24 (OZ: 2024-0.633.166)
Leistungsauftrag gegen den Österreichischen Rundfunk (ORF) wegen www.orf.at

In seiner an die DSB gerichteten Beschwerde wandte sich der Beschwerdeführer, vertreten durch die Datenschutzorganisation NOYB, gegen die Verarbeitung seiner personenbezogenen Daten anlässlich des Besuchs der Website www.orf.at. Auf das Wesentliche zusammengefasst wurde vorgebracht, dass der Cookie-Banner - das Ersuchen um Einwilligung in die Verarbeitung personenbezogener Daten durch das Setzen von Cookies - des Beschwerdegegners nicht den Vorgaben an eine gültige Einwilligung entspreche und seine personenbezogenen Daten (die in den Cookies enthaltenen Werte) zu löschen seien.

Mit Bescheid vom 28. Oktober 2024 wurde die Beschwerde abgewiesen, da die Cookie-Werte im Entscheidungszeitpunkt bereits gelöscht waren. Allerdings hat die DSB von ihren Abhilfebefugnissen Gebrauch gemacht und amtswegig die Anpassung der Website www.orf.at aufgetragen.

Diesbezüglich ist vorauszuschicken ist, dass es sich nach gefestigter Judikatur des BVwG bei den in Cookies enthaltenen Werten (jedenfalls bei Werbe- und Trackingcookies, die eine Datenübermittlung an zahlreiche Drittanbieter zur Folge haben) um personenbezogene Daten handelt und die amtswegige Inanspruchnahme von Abhilfebefugnissen auch in Beschwerdeverfahren nach Art. 77 DSGVO möglich ist.

Der Leistungsauftrag an den Beschwerdegegner bestand aus zwei Punkten: Zunächst wurde aufgetragen, die Option „Alle akzeptieren" in optischer Hinsicht gleichwertig zu gestalten wie die Option „Nur notwendige Cookies". Nach Ansicht der DSB hebt sich die dunkelblaue Schaltfläche „Alle akzeptieren" vom weißen Hintergrund viel deutlicher ab (Kontrastverhältnis 5.42:1) als die hellgraue Schaltfläche „Nur notwendige Cookies" (Kontrastverhältnis 1.13:1). Wenn die Aufmerksamkeit von betroffenen Personen derart prominent auf die Schaltfläche „Alle akzeptieren" gelenkt wird, kann – insbesondere auch im Lichte der strengen Judikatur des EuGH zur Gestaltung von Einwilligungsersuchen – im Ergebnis von keiner gültigen Einwilligung ausgegangen werden.

Darüber hinaus ergab eine Überprüfung der Website www.orf.at, dass noch vor einer Interaktion mit dem Cookie-Banner Cookies gesetzt werden, die aus technischer Sicht nicht erforderlich sind und die (bzw. deren Werte) ebenfalls als personenbezogene Daten nach Art. 4 Z 11 DSGVO zu qualifizieren sind. Da für technisch nicht erforderliche Cookies eine vorherige Einwilligung einzuholen ist und die Bestimmungen des ORF-G nicht als Rechtsgrundlage herangezogen werden können, erging ein diesbezüglicher Leistungsauftrag zur Anpassung der Website. Dieser Bescheid ist nicht rechtskräftig.

6. Bescheid vom 12. Dezember 2024, GZ: D124.1675/24 (OZ: 2024-0.657.101)
Neues Medienprivileg

Gegenstand des Verfahrens war die Frage, ob das Recht auf Löschung des Beschwerdeführers dadurch verletzt wurde, indem die Beschwerdegegnerin die Löschung eines Zeitungsartikels bzw. des darin enthaltenen Namens des Beschwerdeführers verweigert hat. Der Antrag auf Löschung des Artikels bzw. zumindest auf die Entfernung der personenbezogenen Daten des Beschwerdeführers wurde von der Beschwerdegegnerin mit der Begründung abgelehnt, dass Art. 17 DSGVO wegen § 9 Abs. 1 Z 6 lit. b und § 9 Abs. 1 Z 6 lit. c DSG auf die in Rede stehende Verarbeitung der personenbezogenen Daten des Beschwerdeführers nicht anwendbar sei.

Der VfGH hatte mit Erkenntnis vom 14. Dezember 2022, G 287/2022 u.a., § 9 Abs. 1 DSG idF BGBl. I Nr. 24/2018 mit Wirkung vom 30. Juni 2024 als verfassungswidrig aufgehoben. Der inzwischen novellierte § 9 DSG idF BGBl. I Nr. 62/2024 wurde von der DSB der Entscheidung zugrunde gelegt.

Die DSB hat die Beschwerde abgewiesen und entschieden, dass die Beschwerdegegnerin als Medieninhaberin gemäß § 1 Abs. 1 Z 8 MedienG sowie Herausgeberin gemäß § 1 Abs. 1 Z 9 MedienG zu qualifizieren ist. Im konkreten Fall ist § 9 Abs. 1 Z 6 lit. b DSG einschlägig und gemäß dieser Bestimmung sind in Bezug auf personenbezogene Daten, die in einem Medium im Sinne des § 1 Abs. 1 Z 1 MedienG veröffentlicht wurden, die Art. 16 (Recht auf Berichtigung),

Art. 17 (Recht auf Löschung) und Art. 18 (Recht auf Einschränkung der Verarbeitung) DSGVO nicht anzuwenden.

Da der beschwerdegegenständliche Artikel bzw. die darin enthaltenen personenbezogenen Daten des Beschwerdeführers (Vor- und Nachname) in einem Medium veröffentlicht worden sind, dessen Medieninhaberin und Herausgeberin die Beschwerdegegnerin ist, war Art. 17 DSGVO (Recht auf Löschung) gemäß § 9 Abs. 1 Z 6 lit. b DSG nicht anwendbar.

Der Bescheid ist nicht rechtskräftig.

7. Bescheid vom 17. Dezember 2024, GZ: D130.1013 (OZ: 2024-0.743.431)
Datenschutzrechtliche Rollenverteilung und Verantwortlicheneigenschaft für Dienste, die in Zusammenhang mit einem Google-Konto genutzt werden

Die DSB hatte sich in diesem Verfahren u.a. mit der Frage zu beschäftigen, wer für die Verarbeitung personenbezogener Daten bei Diensten, die in Zusammenhang mit einem Google-Konto genutzt werden, als datenschutzrechtlich Verantwortlicher iSd. Art. 4 Z 7 DSGVO anzusehen ist.

Die Beschwerde selbst wurde ausdrücklich gegen die in den USA ansässige Google LLC gerichtet. Im Verfahren wurde die Verantwortlicheneigenschaft der Google LLC bestritten und es wurde darauf verwiesen, dass für alle im EWR angebotenen Google-Dienste die in Irland niedergelassene Google Ireland Limited als datenschutzrechtlich Verantwortliche anzusehen sei.

Die DSB ist diesem Vorbingen nicht gefolgt und hat ausgesprochen, dass bereits aufgrund der allgemeinen Lebenserfahrung davon auszugehen ist, dass nicht kleinere Standorte des Google-Konzerns, sondern die in den USA hauptniedergelassene Muttergesellschaft Google LLC die grundsätzliche Konzernstrategie für Google festlegt und darüber entscheidet, inwiefern die Einführung von Produkten oder Features innerhalb gewisser Märkte angestrebt und eingeleitet werden soll. Dem steht nicht entgegen, dass die praktische Umsetzung lokalen Tochtergesellschaften, wie der Google Ireland Limited, überlassen wird.

Ferner stellte die DSB fest, dass auch die Google Ireland Limited aufgrund ihrer Möglichkeiten der Einflussnahme auf die Ausgestaltung der beschwerdegegenständlichen Verarbeitungsvorgänge, die bei der Nutzung von Diensten in Zusammenhang mit einem Google-Konto anfallen, hinreichende Entscheidungsbefugnisse ausübt.

Unter Verweis auf die mittlerweile gefestigte Rechtsprechung des EuGH zur gemeinsamen Verantwortung und insbesondere auf das Urteil vom 7. März 2024, C-604/22, kam die DSB daher zum Ergebnis, dass betreffend die Nutzung von Diensten in Zusammenhang mit einem Google-Konto sowohl die Google LLC als auch die Google Ireland Limited als gemeinsame datenschutzrechtliche Verantwortliche zu qualifizieren sind. Diese Würdigung erfolgte u.a. vor dem Hintergrund, dass sich die Mitwirkung und die Entscheidungen beider Google-Gesellschaften im Hinblick auf die beschwerdegegenständlich relevante Datenverarbeitung und die damit verbundenen Zwecke und Mittel derart ergänzen, dass die Verarbeitung ohne Mitwirkung der jeweils anderen Stelle nicht denkbar wäre.

Der Bescheid ist nicht rechtskräftig.

8. Bescheid vom 27. Dezember 2024, GZ: D124.0318/22 (OZ: 2024-0.937.775)
Veröffentlichung einer Gerichtsentscheidung im Rahmen von privaten Social Media Profilen kann unter die Haushaltsausnahme fallen

Im gegenständlichen Fall bestand zwischen den Verfahrensparteien ein Verwandtschaftsverhältnis. Auch waren dem Beschwerdeverfahren zahlreiche familiäre Konflikte vorangegangen, welche schließlich in einem gerichtlichen Unterlassungsauftrag gegen die Beschwerdeführer mündeten. Da im gemeinsamen Bekanntenkreis (fälschlicherweise) der Eindruck entstanden war, dass die Klage abgewiesen worden sei, entschlossen sich die Beschwerdegegnerinnen zur Veröffentlichung der Gerichtsentscheidung auf Facebook und Instagram.

Den Kern des darauffolgenden Beschwerdeverfahrens bildete die Frage, ob die Veröffentlichung der Gerichtsentscheidung auf Social Media (noch) von der Ausnahmebestimmung des Art. 2 Abs. 2 lit. c DSGVO („Haushaltsausnahme“) umfasst sein könnte. Nach Durchführung mündlicher Einvernahmen stellte die DSB fest, dass die Social Media Profile „privat“ eingestellt und die Postings daher nur für die rund 400 Facebook-Freund:innen bzw. 300 Instagram-Follower:innen der Beschwerdegegnerinnen ersichtlich waren. Im Rahmen der rechtlichen Beurteilung führte die DSB unter Hinweis auf ErwGr. 18 der DSGVO sowie OGH 6 Ob 56/21k und BVwG W274 2243175-1 aus, dass die Nutzung sozialer Netze grundsätzlich eine ausschließlich persönliche oder familiäre Tätigkeit darstellen kann, sofern lediglich ein begrenzter Benutzer:innenkreises vorliegt und das Profil ausschließlich zu privaten Zwecken genutzt wird. Bei Vorhandensein dieser Voraussetzungen schadet selbst ein nicht unerheblich großer Follower:innenkreis nicht. Im Ergebnis war die Geheimhaltungsbeschwerde aufgrund der Anwendbarkeit des Art. 2 Abs. 2 lit. c DSGVO abzuweisen. Dieser Bescheid ist nicht rechtskräftig.

4.2.1.2 Grenzüberschreitende Fälle der DSB

Die DSB behandelt neben nationalen Verfahren auch grenzüberschreitende Fälle. Diese umfassen sowohl von Betroffenen erhobene Beschwerden und amtswegige Prüfverfahren, als auch Mitteilungen über Sicherheitsverletzungen gemäß Art. 33 DSGVO.

Bei grenzüberschreitenden Fällen ist danach zu unterschieden, ob die DSB das Verfahren alleine führt und am Ende eine materielle Entscheidung erlässt, oder ob eine Zuständigkeit weiterer Aufsichtsbehörden gegeben ist.

Wurde die Beschwerde bei der DSB eingebracht und richtet sie sich gegen eine:einen Verantwortliche:n oder Auftragsverarbeiter:in, der:die in einem anderen Mitgliedstaat des EWR[12] niedergelassen ist, dann ist in der Regel ein sog. **One-Stop-Shop Verfahren gemäß Art. 56 DSGVO iVm. Art. 60 DSGVO** zu führen.[13] An einem solchen Verfahren sind in weiterer Folge die federführende Aufsichtsbehörde sowie die betroffenen Aufsichtsbehörden beteiligt. Eine Federführung der DSB liegt grundsätzlich dann vor, wenn eine Beschwerde in einem anderen Mitgliedstaat erhoben wird und sich gegen eine:einen Verantwortliche:n oder Auftragsverarbeiter:in mit Hauptniederlassung in Österreich richtet.

Hat eine:ein Verantwortliche:r oder ein:eine Auftragsverarbeiter:in **keine Niederlassung bzw. keinen Sitz in einem anderen Mitgliedstaat des EWR**, so kann dennoch der räumliche An-

12 EU-Mitgliedstaaten sowie Norwegen, Island und Liechtenstein.
13 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.

wendungsbereich der DSGVO aufgrund des sog. **Marktortprinzips**[14] eröffnet sein und die DSB ist dann selbst für die Verfahrensführung zuständig.

Bei der DSB wurden im Berichtsjahr 2024 insgesamt **600 grenzüberschreitende Beschwerden eingebracht**. In 511 Fällen richteten sich die Beschwerden gegen Verantwortliche mit Sitz in einem anderen Mitgliedstaat im EWR und es wurde in diesen Fällen ein One-Stop-Shop Verfahren eröffnet. In **89** Fällen wurden bei der DSB **Beschwerden gegen Verantwortliche oder Auftragsverarbeiter:innen,** welche **in einem Drittland** niedergelassen sind, anhängig gemacht und die DSB hat in 32 Fällen mit Drittlandsbezug eine verfahrenserledigende Erledigung erlassen.

Umgekehrt sind bei der DSB im Berichtsjahr 2024 insgesamt 856 grenzüberschreitende Beschwerden, welche im Ausland eingebracht wurden, eingelangt und die DSB hat sich in 175 Fällen als betroffene Aufsichtsbehörde und in 19 Fällen als federführende Aufsichtsbehörde gem. Art. 56 DSGVO deklariert.

Im Rahmen der grenzüberschreitenden Zusammenarbeit innerhalb und außerhalb eines konkreten Verfahrens machte die DSB **199 Mal v**on der **gegenseitigen Amtshilfe iSd. Art. 61 DSGVO** Gebrauch und wurde selbst i**n 612 Fällen von anderen Aufsichtsbehörden kontaktiert**.

Bei Uneinigkeiten zwischen Aufsichtsbehörden im Rahmen grenzüberschreitender Verfahren sieht **Art. 65 DSGVO** ein Streitbeilegungsverfahren vor dem EDSA vor, welcher mittels verbindlichem Beschluss über den Streitfall entscheiden kann. Ferner kann unter außergewöhnlichen Umständen auf begründeten Antrag einer Aufsichtsbehörde ein Dringlichkeitsverfahren vor dem EDSA geführt werden. Im Jahr 2024 wurden weder Verfahren zur Streitbeilegung iSd. Art. 65 Abs. 1 lit. a DSGVO, noch Dringlichkeitsverfahren iSd. **Art. 66 Abs. 2 und 3 DSGVO** vor dem EDSA anhängig gemacht.

Ein Überblick über ausgewählte grenzüberschreitende Beschwerdeverfahren wird in **Kapitel 4.2.1.1.** gegeben.

4.2.2 Rechtsauskünfte an Bürgerinnen und Bürger

Die DSB stellt auf ihrer **Webseite** (abrufbar unter: https://dsb.gv.at/faq/faqs und unter https://dsb.gv.at/faq/faqs-zum-thema-ki-und-datenschutz), in leicht verständlicher und benutzerfreundlicher Form, **umfassende Informationen im Zusammenhang mit dem geltenden Datenschutzrecht** zur Verfügung. Hierbei handelt es sich um Antworten auf die relevantesten datenschutzrechtlichen Fragen. Ein Leitfaden zur DSGVO, der anlassbezogen aktualisiert wird, ist ebenso auf der Webseite abrufbar (https://dsb.gv.at/sites/site0344/media/downloads/dsgvo_leitfaden_2022.pdf).

Zusätzlich verschafft die DSB auf ihrer Startseite unter **„aktuelle Bekanntmachungen der DSB“** (abrufbar unter: www.dsb.gv.at) einen raschen Überblick über die neuesten Entwicklungen im Datenschutzrecht. Darüber hinaus beantwortet die DSB **allgemeine Anfragen** zum geltenden Datenschutzrecht sowohl **schriftlich, als auch telefonisch**. Telefonische Rechtsauskünfte werden während der Amtsstunden erteilt.

14 Art. 3 Abs. 2 DSGVO, bspw. bei einem Anbieten von Waren oder Dienstleistungen an betroffene Personen in der Union.

Die DSB nimmt im Rahmen der Beantwortung von Anfragen grundsätzlich keine Vorabprüfung hinsichtlich der Unzulässigkeit bzw. 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 DSB, präjudizieren würde.

Ferner finden sich auf der Webseite der DSB ausführliche Informationen über die Rechte der betroffenen Personen und die Zuständigkeit der DSB (abrufbar unter: https://dsb.gv.at/rechte-pflichten/ihre-rechte-als-betroffene-person).

Ein **Newsletter** über Bekanntmachungen und aktuelles, der mindestens vierteljährlich erscheint, informiert unter anderem über ausgewählte Entscheidungen der DSB, ausgewählte Entscheidungen der Gerichte und die aktuelle Rechtsprechung.

4.2.3 Genehmigungen im Internationalen Datenverkehr

Die DSGVO sieht weitgehend eine Genehmigungsfreiheit für den internationalen Datenverkehr an Empfänger:innen außerhalb des EWR vor. Die Übermittlung personenbezogener Daten an Empfänger:innen in Drittländern oder in internationalen Organisationen ist in **Kapitel V DSGVO** geregelt. Sofern für den jeweiligen Zielort der Datenübermittlung kein Angemessenheitsbeschluss[15] der Europäischen Kommission besteht, sieht **Art. 46 DSGVO unterschiedliche rechtliche Instrumente zur Sicherstellung eines angemessenen Datenschutzniveaus**[16] vor.

Grundsätzlich ist eine Genehmigung dieser Instrumente durch die zuständige Datenschutzaufsichtsbehörde nur mehr in bestimmten Fällen 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** der EDSA zu befassen.

Eine weitere Ausnahme bilden die sog. **„Verbindlichen internen Datenschutzvorschriften"**[17] (**Binding Corporate Rules – BCRs**), welche von der zuständigen Datenschutzaufsichtsbehörde unter Anwendung des **Kohärenzverfahrens gemäß Art. 63 ff. DSGVO** genehmigt werden.[18] Hierbei ist eine enge Zusammenarbeit mit den anderen europäischen Datenschutzaufsichtsbehörden im Rahmen des EDSA notwendig.[19] Aufgrund dieses Abstimmungsprozesses und 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

15 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.

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

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

18 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* sowie dem Working Document on Binding Corporate Rules for Processors, WP257/rev.01 der ehemaligen *Artikel-29-Datenschutzgruppe* zu entnehmen, welches einer Überarbeitung unterzogen wird

19 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.

abgewogen werden, ob die Zulässigkeit der Datenübermittlung nicht einfacher und effizienter durch andere geeignete Garantien im Sinne des **Art. 46 Abs. 2 DSGVO**, wie etwa durch die modularen Standarddatenschutzklauseln der Europäischen Kommission[20] , erreicht werden kann.[21] 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.[22]

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.[23] Auch in diesen Fällen ist eine Befassung des EDSA sowie der Europäischen Kommission vorgesehen.[24]

Bei der DSB wurden im Jahr 2024 keine neuen Genehmigungsverfahren nach Kapitel V DSGVO anhängig gemacht. Im selben Zeitraum hat sich die DSB in einem Fall als *„Co-Reviewer"* von genehmigungspflichtigen Garantien iSv. Kapitel V DSGVO, die bei einer anderen Datenschutzaufsichtsbehörde eingebracht wurden, beteiligt.

4.2.4 Genehmigungen nach §§ 7 u. 8 DSG

§ 7 DSG regelt die Voraussetzungen für die V**erarbeitung personenbezogener Daten für archivarische, wissenschaftliche, historische oder statistische Zwecke**.

§ 8 DSG legt die Voraussetzungen für die **Zurverfügungstellung von Adressdaten zum Zweck der Benachrichtigung/Befragung des Betroffenen aus wichtigem Interesse selbst, aus wichtigem öffentlichen Benachrichtigungs- und Befragungsinteresse oder zur Befragung des Betroffenen für wissenschaftliche oder statistische Zwecke** fest.

Entscheidungen der DSB im Jahr 2024

Im Rahmen der **§§ 7 und 8 DSG** langten bei der DSB im Jahr 2024 insgesamt **13 Anträge** ein.

Hinsichtlich **§ 7 Abs. 3 DSG** ist die Entscheidung der DSB vom 6. Juni 2024 zu **GZ: D202.337 (OZ: 2024-0.373.701)** hervorzuheben, mit der die DSB dem Antrag auf Auswertung von Videoaufzeichnungen im Bereich der Fahrgastströme in öffentlichen Verkehrsmitteln zur Optimierung der Auslastung von Schienenfahrzeugen stattgegeben hat. Zu diesem Zweck wurde

20 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.

21 Es ist darauf hinzuweisen, dass die Europäische Kommission die Erlassung eines weiteren Sets von Standardvertragsklauseln für Drittlandsverantwortliche und -auftragsverarbeiter, die der DSGVO unterliegen, in Aussicht gestellt hat. Der aktuelle Stand des Vorhabens ist in deutscher Sprache abrufbar unter *https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14404-Standardvertragsklauseln-fur-die-Ubermittlung-von-Daten-an-Verantwortliche-und-Auftragsverarbeiter-in-Drittlandern-die-der-Datenschutz-Grundverordnung-DSGVO-unterliegen_de*.

22 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*.

23 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*, Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen, Version 2.0, abrufbar in deutscher Sprache unter https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_de_0.pdf.

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

den Antragstellern genehmigt, pseudonymisierte und anonymisierte Videoaufzeichnungen aus einem ausdrücklich als Testwagen gekennzeichneten Fahrzeug der Wiener Linien GmbH & Co. KG für Forschungszwecke zur Auslastungsoptimierung im Schienenverkehr im Rahmen eines Forschungsprogramms an Standorten in Wien zu verarbeiten. Neben dem Vorliegen der sonstigen Voraussetzungen des § 7 Abs. 3 DSG war insbesondere auch das zusätzliche Kriterium des wichtigen öffentlichen Interesses an der Untersuchung erfüllt, da das Forschungsprojekt u.a. die Verbesserung der Auslastung von Schienenfahrzeugen, insbesondere für Personen mit Behinderungen, wie z.B. Rollstuhlfahrer:innen oder Personen mit eingeschränkten Sehfunktionen, zum Ziel hat.

Mit Bescheid über die Erteilung einer Genehmigung gemäß **§ 8 Abs. 3 und 4 DSG** vom 13. Mai 2024 zu **GZ: D202.336 (OZ: 2024-0.288.493)** wies die DSB den Antrag der Antragstellerin, einer Stadt, zurück. Die Stadt ersuchte die DSB um Genehmigung der Übermittlung personenbezogener Daten aller Schüler:innen einer Pflichtschule an ein Beteiligungsunternehmen der Antragstellerin. Durch die Verwendung der Daten aus der Schulpflichtmatrik könne auf validierte Registerdaten zurückgegriffen werden, was die Kontaktaufnahme mit den Erziehungsberechtigten ermögliche. Ziel war es dabei, den Erziehungsberechtigten vorausgefüllte Antragsformulare zur Beantragung der sogenannten Schülerfreifahrt zu übermitteln, um Warteschlangen bei regelmäßigen Spitzenbelastungen und Rechtschreibfehler oder Unleserlichkeit der Angaben zu vermeiden. Gemäß § 8 Abs. 1 DSG muss es sich dabei um Adressdaten eines bestimmten Kreises von Betroffenen zum Zweck der Benachrichtigung oder der Einholung der Einwilligung der Betroffenen handeln. Dementsprechend waren nach § 8 Abs. 4 DSG grundsätzlich nur die Adressdaten der Erziehungsberechtigten genehmigungsfähig. Eine Beeinträchtigung der Geheimhaltungsinteressen der Erziehungsberechtigten war nicht zu erwarten, zumal keine besonderen Kategorien personenbezogener Daten verarbeitet werden sollten, weshalb eine diesbezügliche Genehmigung des Antrags durch die DSB gemäß § 8 Abs. 3 iVm Abs. 4 DSG nicht erforderlich und der Antrag daher hinsichtlich der Übermittlung der Adressdaten der Erziehungsberechtigten zurückzuweisen war.

4.2.5 Amtswegige Prüfverfahren

Die DSB erhielt im Jahr 2024 **1066 Anzeigen und Anregungen** zur Einleitung amtswegiger Prüfverfahren. Im Berichtszeitraum wurden **796 amtswegige Prüfverfahren durch Bescheid, Einstellung oder Sensibiliserungsschreiben erledigt**. Weitere 188 Verfahren wurden auf Verfahrensarten (zB. Beschwerdeverfahren) umprotokolliert. Daher ergeben sich 646 Verfahren, welche als neue amtswegige Prüfverfahren geführt werden und 504 Verfahren wurden im Berichtszeitraum abgeschlossen.

Ausgewählte Entscheidungen:

1. Bescheid vom 24. April 2024, OZ: 2024-0.026.783 (GZ: D213.2328)
Prüfverfahren zu („anonymisierten") Schwangerschaftsabbruchsregistern, Warnung gemäß Art. 58 Abs. 2 lit. a DSGVO

Aufgrund verschiedener Medienberichte im September 2023 über zwei Bundesländer, die ein *„Schwangerschaftsabbruchregister"* planen würden, leitete die DSB jeweils ein amtswegiges Prüfverfahren zur datenschutzrechtlichen Überprüfung gegen das Amt der jeweiligen Landesregierung gemäß Art. 57 Abs. 1 lit. h iVm Art. 58 Abs. 1 lit. b DSGVO iVm § 22 Abs. 1 DSG ein.

Eines der beiden amtswegigen Prüfverfahren konnte bereits zu Beginn des Ermittlungsverfahrens eingestellt werden, da das Büro des Landesamtsdirektors dieses Bundeslandes mitteilte, dass kein Schwangerschaftsabbruchregister geplant sei.

Im anderen Prüfverfahren teilte das Amt der Landesregierung mit, dass das Land für dieses lediglich eine Förderung im Rahmen der Wissenschaftsförderung des Landes zur Verfügung stelle und die Projektleitung bzw. Verantwortlichkeit nicht beim Land angesiedelt sei. Beim Projekt handle es sich um ein Projekt der Krankenhausträgergesellschaft. Daraufhin erweiterte die DSB die Datenschutzüberprüfung auf die Krankenhausträgergesellschaft.

Verfahrensgegenständlich haben die Ermittlungen der DSB ergeben, dass das beabsichtigte Schwangerschaftsabbruchregister von der Krankenhausträgergesellschaft (als Auftragsverarbeiter) betrieben werden soll und vorgesehen ist, dass die in das Register einmeldenden Arztpraxen bzw. Kliniken als Verantwortliche des Registers fungieren. Die Datenerfassung erfolge anonym und diene dem Ziel, Versorgungsengpässe bzw. die Risiken für Schwangerschaftsabbrüche und Teenagerschwangerschaften zu identifizieren.

Aus den durch die Erhebung erfassten Kategorien von Daten ergaben sich erhebliche Zweifel an der Anonymisierung, dem Zweck der Verarbeitung und an der Rollenverteilung. So gab es Zweifel daran, ob die Aggregation der Gesundheitsdaten nach Alterskohorten für eine Anonymisierung – dh. eine vollständige Beseitigung eines möglichen Personenbezugs – in allen Fällen zureichend ist. Ebenso erschienen die übergeordneten Zwecke der Verarbeitung eines Schwangerschaftsabbruchregisters (etwa Versorgungsengpässe im Land) mit den Aufgaben der „Alleinverantwortlichen“ (einmeldende Arztpraxen bzw. Kliniken) nicht vereinbar.

Aufgrund dessen sprach die DSB mit Bescheid eine Warnung gemäß Art. 58 Abs. 2 lit. a DSGVO an Verantwortliche und Auftragsverarbeiter insofern aus, als die beabsichtigte Verarbeitung mangels geeigneter Rechtsgrundlage und aufgrund der beabsichtigen Rollenverteilung voraussichtlich Bestimmungen der DSGVO widerspricht.

Der Bescheid ist rechtskräftig.

2. Bescheid vom 11. September 2024, OZ: 2024-0.292.722 (GZ: D213.2761)
Newsletter-Zustellung ohne Einwilligung durch eine Wähler:innengruppe, Warnung gemäß Art. 58 Abs. 2 lit. b DSGVO

Dieses amtswegige Prüfverfahren wurde aufgrund einer anonymen Anzeige eingeleitet und führte zu einer Verwarnung einer in einem Gemeinderat vertretenen Wähler:innengruppe (Wahlpartei, Liste).

Diese hatte einen Initiativantrag gemäß § 16 NÖ-Gemeindeordnung betreffend eine Gebührensenkung initiiert und dazu Vor- und Nachname, Adresse, Unterschrift sowie E-Mail-Adresse von Unterstützer:innen erhoben. Obwohl keine ausdrückliche Einwilligungserklärung vorlag, wurden die erhobenen E-Mail-Adressen anschließend für die Zusendung eines Newsletters über die (politische) Tätigkeit der Verantwortlichen verwendet. Im Laufe des Verfahrens vor der DSB wurden diese Daten gelöscht.

In rechtlicher Hinsicht führte die DSB zunächst aus, dass die Wähler:innengruppe auch als nach hM nur beschränkt rechtsfähige Wahlpartei (wahlwerbende Partei im Sinne des § 2 Z 2 PartG) als für die Verarbeitung Verantwortliche in einem Prüfverfahren passiv legitimiert ist. Verfahrensgegenständlich konnte die bloße Unterstützungserklärung des Initiativantrags nicht

als (rechtsgültige) Einwilligung iSd. Art. 6 Abs. 1 lit. a iVm Art. 7 DSGVO qualifiziert werden. Insbesondere fehlte es an entsprechenden Informationen („Treu und Glauben“) und an einer eindeutigen bestätigenden Handlung. Auch konnte sich die Verantwortliche nicht auf eine von ihr vorgebrachte „konkludente Einwilligung“ stützen. Eine solche Einwilligung ist der DSGVO nämlich fremd (ErwGr. 32 der DSGVO). Aber auch eine ausdrückliche Einwilligung wäre wegen fehlender Trennung von der Unterstützung des politischen Anliegens (Verstoß gegen Art. 7 Abs. 2 DSGVO) nicht wirksam gewesen.

Deswegen erfolgte die verfahrensgegenständliche Verarbeitung ohne Rechtsgrundlage und die DSB sprach wegen des Verstoßes gegen Art. 5 Abs. 1 lit. a iVm Art. 6 Abs. 1 DSGVO eine Verwarnung aus, da die Verarbeitung vor Bescheiderlassung bereits beendet worden war.

Der Bescheid ist rechtskräftig.

4.2.5.1 Schwerpunktprüfung 2024

Die DSB hat im Jahr 2024 eine **Schwerpunktprüfung im Telekomsektor** durchgeführt. Insgesamt wurden **10 Unternehmen** datenschutzrechtlich überprüft.

Der Fokus der Prüfungen lag in der Einhaltung allgemeiner Verpflichtungen wie der Grundsätze für die Verarbeitung personenbezogener Daten nach **Art. 5 DSGVO**, technischer und organisatorischer Maßnahmen zur Sicherheit der Datenverarbeitung, der Übermittlung von personenbezogenen Daten in Drittländer oder der Stellung des Datenschutzbeauftragten. Dabei wurde, wie in den Jahren zuvor, das sogenannte **„Coordinated Enforcement Framework“ (CEF)** – eine jährlich stattfindenden koordinierten Prüftätigkeit europäischer Datenschutzbehörden – miteinbezogen. Das CEF hatte im Jahr 2024 das **Recht auf Auskunft nach Art. 15 DSGVO** zum Gegenstand.[25] Anhand eines von den europäischen Datenschutzbehörden gemeinsam erarbeiteten Fragebogens wurden sohin auch detaillierte Fragen zur Modalität der Auskunftserteilung, zum sogenannten Recht auf Erhalt einer Kopie (**Art. 15 Abs. 3 DSGVO**) oder zur möglichen Einschränkung von Auskunftsanträgen an die geprüften Unternehmen gestellt.

Im Rahmen der Prüfverfahren ergaben sich teilweise Rückfragen an die Unternehmen. Punktuelle Verbesserungsvorschläge seitens der DSB wurden umgesetzt, sodass keine bescheidmäßige Anweisung erforderlich war. Insgesamt konnte daher eine positive Bilanz gezogen werden.

Auch für das Jahr 2025 ist eine Schwerpunktprüfung geplant.

4.2.6 Beschwerdeverfahren vor dem BVwG, einschließlich Säumnisbeschwerden

1. Erkenntnisse vom 27. März 2024, W214 2243436-1 und 07. Juni 2024, W256 2246230-1
Verwaltungsstrafverfahren wegen zwei unterschiedlichen Kundenbindungsprogrammen

Die DSB hat im Jahr 2021 unter anderem zwei Straferkenntnisse in Höhe von EUR 1,2 Millionen und EUR 2 Millionen gegen zwei Verantwortliche verhängt, die in Österreich jeweils ein Kundenbindungsprogramm betrieben haben, wegen der unrechtmäßigen Verarbeitung personen-

25 https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_de.

bezogener Daten. Die von den Verantwortlichen ins Treffen geführte Einwilligung der betroffenen Personen für die Verarbeitung zum Zwecke von Profiling wurde als nicht zulässig erachtet, weil die Formulare (physische Flyer oder über eine digitale Anmeldestrecke auf der Webseite der Verantwortlichen) zur Erhebung dieser Einwilligungen nach Ansicht der DSB irreführend gestaltet waren. Mangels rechtskonformer Einwilligung durch die betroffenen Personen konnte die darauf aufbauende Verarbeitung daher nicht als rechtmäßig erachtet werden.[26]

Das BVwG setzte sich mit den gegen die Straferkenntnisse erhobenen Beschwerden der Verantwortlichen auseinander und bestätigte im Rahmen der oben genannten Verfahren im Wesentlichen die Ansicht der DSB, wonach es sich um unzulässige Einwilligungen handelt, weil die Formulare irreführend gestaltet waren. Die darauf aufbauende Verarbeitung sei daher unrechtmäßig erfolgt und die Verantwortlichen hätten schuldhaft gehandelt. Im Ergebnis hätten sie daher die von der DSB vorgeworfenen Verwaltungsübertretungen zu verantworten.

In beiden Fällen nahm das BVwG jedoch im eigenen Ermessen eine neue Strafzumessung vor und gelangte zum Ergebnis, dass die Geldbuße im ersten Fall von EUR 1,2 Millionen auf EUR 700.000 und im zweiten Fall von EUR 2 Millionen auf EUR 500.000 aufgrund der näher festgestellten Umstände zum Zeitpunkt der Entscheidung des Gerichts herabgesetzt werden müsse, damit eine tat- und schuldangemessene Sanktion angenommen werden kann.

Die Revision wurde zugelassen, jedoch sah die Verantwortliche im ersten Fall von der Erhebung weiterer Rechtsmittel ab und akzeptierte die Geldstrafe. Im zweiten Fall wurde jedoch sowohl von der Verantwortlichen als auch von der DSB (wegen der Strafhöhe) eine Revision beim VwGH eingebracht. Das Revisionsverfahren ist derzeit noch anhängig.

2. Erkenntnis vom 5. Juli 2024, W292 2284228-1/49E
Entscheidung im Fall „GIS Data Breach“

Bei der DSB wurden im Verlauf des Jahres 2023 rund 200 Datenschutzbeschwerden erhoben, die gegen die damalige GIS – Gebühren Info Service GmbH (nunmehr: ORF-Beitrags Service GmbH) gerichtet waren. Gegenstand dieser Datenschutzbeschwerden war der sogenannte „GIS Data Breach“. Zusammengefasst handelt es sich um einen Vorfall aus dem Jahre 2020, im Zuge dessen Meldedaten der österreichischen Bevölkerung im Darknet zum Verkauf angeboten wurden. Diese Meldedaten wurden von einem Hacker zugänglich gemacht, der nach den Feststellungen der DSB diese Daten von einem seitens der (damals) GIS beauftragten IT-Unternehmen rechtswidrig erbeutet hatte.

Die DSB gelangte in den meisten Verfahren zu dem Ergebnis, dass die jeweils beschwerdeführende Partei von dem gegenständlichen Vorfall betroffen ist. Das bedeutet, dass die Meldedaten der beschwerdeführenden Partei zum damaligen Zeitpunkt entwendet und in weiterer Folge im Darknet entgeltlich angeboten worden waren. Sofern in diesen Fällen eine Verletzung im Recht auf Geheimhaltung oder die Rechtmäßigkeit der Datenverarbeitung geltend gemacht wurde, stellte die DSB einen entsprechenden Verstoß der (damals) GIS gegen datenschutzrechtliche Bestimmungen bescheidmäßig fest. Die Feststellung gründet darauf, dass das seitens der GIS beauftragte IT-Unternehmen nach Ansicht der DSB unzureichende Sicherheitsmaßnahmen im Sinne des Art. 32 DSGVO implementiert hat. Darüber hinaus ist ein Fehlverhalten des Auftragsverarbeiters dem Verantwortlichen zuzurechnen.

26 Siehe im Detail die Ausführungen im Datenschutzbericht 2021, Punkt 3.2.10, S. 50 *„Unzulässige Einwilligungen/Verarbeitung im Rahmen von Kundenbindungsprogrammen“.*

Das BVwG wurde in weiterer Folge anlässlich einer Bescheidbeschwerde befasst. In zumindest einem Fall wurde der Bescheid der DSB – und die darin vertretenen Rechtsansichten – bestätigt. Insbesondere hatte das BVwG auch keine Bedenken, das Verfahren gegen die nunmehrige OBS weiterzuführen, da es sich bei dieser um dieselbe Gesellschaft (bzw. Behörde) handle. Dieses Erkenntnis ist formell rechtskräftig, allerdings wurde dagegen Revision an den VwGH erhoben, wobei der Revision keine aufschiebende Wirkung zukommt.

3. Erkenntnis vom 28.August.2024, W221 2279014-1/25E
Für das Vorliegen einer Datenverarbeitung trägt der Beschwerdeführer die Beweislast

Im vorliegenden Fall hatte das BVwG die Frage zu beurteilen, ob die in einem Tesla-Fahrzeug verbauten Videokameras zu einem bestimmten Zeitpunkt aktiv waren und daher den Beschwerdeführer filmten oder nicht (so genannter „Wächtermodus"). Die DSB hatte mit Teilbescheid vom 13. September 2023, D124.3884, die Beschwerde wegen Verletzung in den Rechten auf Information und auf Geheimhaltung als unbegründet abgewiesen, weil die Videokameras nicht aktiv gewesen seien. Es war somit vom BVwG die Frage zu klären, ob überhaupt eine Datenverarbeitung vorlag. Der Beschwerdeführer brachte vor, dass es ihm nicht möglich sei, zu beweisen, dass die Kameras tatsächlich aktiv waren. Vielmehr müsse der Beschwerdegegner beweisen, dass er keine Datenverarbeitung vorgenommen habe.

Das BVwG führte unter Heranziehung von EuGH-Rechtsprechung aus, dass ein Verantwortlicher die Beweislast für die Rechtmäßigkeit der Datenverarbeitung iSd Art. 5 DSGVO trägt. In Bezug auf das Vorliegen einer Datenverarbeitung finden sich jedoch weder in Rechtsprechung, noch in Normen Hinweise auf eine entsprechende Beweislastumkehr. Daher ist für den Umstand, ob überhaupt eine Datenverarbeitung vorliegt, der Beschwerdeführer beweispflichtig.

Dieses Erkenntnis ist rechtskräftig.

4. Erkenntnis vom 25. Oktober 2024, W101 2256689-1/5E
Art. 19 DSGVO: Pflicht des Verantwortlichen, den BF über Löschung oder Berichtigung von sich aus VOR dem Verfahren vor DSB zu informieren

Der Beschwerdeführer (im Ausgangsverfahren vor der DSB) sah sich im Recht auf Information, auf Löschung und auf Mitteilung einer Berichtigung bzw. Löschung verletzt, da es zu unberechtigten Forderungsbetreibungen gekommen sei. Ursächlich dafür sei gewesen, dass die mitbeteiligte Partei (vormals Beschwerdegegner) eine unrichtige Adresse des Beschwerdeführers verarbeitet habe.

Die mitbeteiligte Partei sei ihrer Mitteilungspflicht gegenüber den Empfängern (der unrichtigen Daten des Beschwerdeführers) gemäß Art. 19 DSGVO erst nach ca. zwei Jahren nachgekommen. Die mitbeteiligte Partei habe den Beschwerdeführer nicht wie von ihm verlangt über die erfolgte Mitteilung an die Empfänger informiert. Die Informationen habe er erst über die DSB durch ihre Mitteilung vom 23. September 2020 und vom 19. Mai 2021 erhalten. Daher begehrte der Beschwerdeführer die Feststellung, dass er im Recht auf Mitteilung nach Art. 19 DSGVO verletzt worden sei.

Im vorangegangenen Teilbescheid vom 20. August 2020, GZ: D124.719 2020-0.427.545, gab die DSB der Datenschutzbeschwerde vom 29. Jänner 2019 wegen einer Verletzung im Recht auf Geheimhaltung statt und stellte fest, dass die mitbeteiligte Partei den Beschwerdeführer im Recht auf Geheimhaltung verletzt hat, indem diese unrichtige personenbezogene Daten - unrichtige

Anschrift und unrichtiger Forderungsbetrag – über den Beschwerdeführer gespeichert und im Rahmen einer Bonitätsauskunft übermittelt hat.

Mit (End-)Bescheid vom 19. Mai 2022, GZ: D124.719 2021-0.476.789, wies die DSB die Datenschutzbeschwerde vom 29. Jänner 2019 u.a. hinsichtlich einer Verletzung des Rechts auf Information (Spruchteil 2.), hinsichtlich einer Verletzung des Rechts auf Löschung (Spruchteil 3.) und hinsichtlich einer Verletzung des Rechts auf Mitteilung einer Berichtigung bzw. Löschung (Spruchteil 4.) ab.

Dieser (End-)Bescheid war nun Gegenstand des Verfahrens vor dem BVwG.

Die DSB hatte die Abweisung dieses Vorbringens in der Datenschutzbeschwerde darauf gestützt, dass die mitbeteiligte Partei ihrer Mitteilungspflicht während des laufenden Verfahrens nachgekommen sei und daher auch hier der Beschwerdeführer durch Beseitigung der Beschwer gemäß § 24 Abs. 6 DSG klaglos gestellt worden sei.

Das BVwG entschied, dass ähnlich der Bestimmung des Art. 14 DSGVO die Bestimmung des Art. 19 DSGVO gerade nicht vom Antrag einer betroffenen Person abhängig ist und eine Pflicht des Verantwortlichen zum eigenständigen Tätigwerden verbürgt.

Insofern ist diese Datenschutzverletzung des Art. 19 DSGVO mit der durch das Erkenntnis des Verwaltungsgerichtshofes Ro 2022/04/0001 klargestellten Rechtslage im Fall der Verletzung im Recht auf Geheimhaltung nach § 1 Abs. 1 DSG vergleichbar. Auch § 24 Abs. 5 zweiter Satz DSG sieht einen (an Verantwortliche des privaten Bereichs gerichteten) Auftrag nur bezüglich der Anträge des Beschwerdeführers auf Auskunft, Berichtigung, Löschung, Einschränkung oder Datenübertragung vor. Eine nachträgliche Beseitigung der Rechtsverletzung bzw. ein darauf gerichteter Auftrag an den Verantwortlichen im Zusammenhang mit dem Recht auf Mitteilung nach Art. 19 DSGVO wurde hingegen nicht angesprochen.

Im Ergebnis ist die mitbeteiligte Partei ihrer Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten des Beschwerdeführers nicht nachgekommen. Daher wurde der Bescheidbeschwerde hinsichtlich der Spruchteils 2 wegen einer Verletzung im Recht auf Information stattgegeben und es wurde festgestellt, dass die mitbeteiligte Partei als Verantwortliche bis 15.11.2018 gegenüber dem Beschwerdeführer ihre Informationspflicht gemäß Art. 14 DSGVO verletzt hat.

Darüber hinaus wurde der Bescheidbeschwerde gegen Spruchteil 4. wegen einer Verletzung im Recht auf Mitteilung einer Berichtigung bzw. Löschung stattgegeben und es wurde festgestellt, dass die mitbeteiligte Partei als Verantwortliche gegenüber dem Beschwerdeführer hinsichtlich der erfolgten Löschung einer unrichtigen Adresse ihre Mitteilungspflicht gemäß Art. 19 DSGVO hinsichtlich der Empfänger verletzt hat.

5. Erkenntnis vom 22.November.2024, W211 2272744–1/9E „Mitwirkungspflicht“ der mitbeteiligten Partei bei der Sachentscheidung

Mit Erkenntnis vom 22. November 2024, GZ: W211 2272744–1/9E, befasste sich das BVwG mit der Frage der „Mitwirkungspflicht“ der mitbeteiligten Partei (ursprünglich beschwerdeführende Partei vor der DSB) bei der Sachentscheidung.

Die nunmehr mitbeteiligte Partei brachte im Verfahren vor der DSB zusammengefasst vor, sie habe ein Impfaufforderungsschreiben vom Beschwerdegegner erhalten und erachte die damit

verbundene Datenverwendung ihrer medizinischen Daten als eklatanten Verstoß gegen den Datenschutz. Sie machte dabei eine Verletzung von § 1 DSG sowie der Art. 5, 6 und 9 DSGVO geltend. Der Datenschutzbeschwerde war kein Impferinnerungsscheiben, das persönlich an die mitbeteiligte Partei gerichtet war, beigefügt. Die DSB gab der Beschwerde schlussendlich statt, wogegen die beschwerdeführende Partei eine Bescheidbeschwerde an das BVwG erhob.

Das BVwG forderte die ursprünglich beschwerdeführende Partei auf, das gegenständliche Impfschreiben vorzulegen, worauf diese nicht reagierte. Daher stellte das BVwG fest, dass nicht festgestellt werden kann, dass die mitbeteiligte Partei ein an sie adressiertes Impferinnerungsschreiben erhalten hat. Dazu führte das BVwG ua. Folgendes aus: *„Fehlt es hingegen an einer hinreichend deutlichen Anordnung (etwa, dass einem Antrag auf Verleihung der österreichischen Staatsbürgerschaft eine Geburtsurkunde aus dem Heimatstaat anzuschließen ist), so kommt bei deren Nichtvorlage weder die Erteilung eines Verbesserungsauftrages noch – nach fruchtlosem Verstreichen der zu Unrecht gesetzten Frist – die Zurückweisung des Anbringens in Frage. Vielmehr kann die unterlassene Beibringung von Unterlagen, welche die Behörde benötigt und die sie sich nicht selbst beschaffen kann, allenfalls – als Verletzung der „Mitwirkungspflicht" – bei der Sachentscheidung Berücksichtigung finden (vgl. Hengstschläger/Leeb, AVG § 13 Rz 27 [Stand 1.1.2014, rdb.at]). Dort, wo es der Behörde nicht möglich ist, den entscheidungswesentlichen Sachverhalt ohne Mitwirkung der Partei festzustellen, ist somit von einer Mitwirkungspflicht der Partei auszugehen. Die Mitwirkungspflicht der Partei ist gerade dort von Bedeutung, wo ein Sachverhalt nur im Zusammenwirken mit der Partei geklärt werden kann, weil die Behörde außerstande ist, sich die Kenntnis von ausschließlich in der Sphäre der Partei liegenden Umständen von Amts wegen zu beschaffen (vgl. VwGH 25.05.2022, Ra 2022/02/077 Rn 14). Eine erhöhte Mitwirkungspflicht nimmt der VwGH grundsätzlich dann an, wenn es um Umstände geht, die in der persönlichen Sphäre der Parteien liegen (vgl. Hengstschläger/Leeb, AVG § 39 Rz 9 ff [Stand 01.04.2021, rdb.at]). Die Mitwirkungspflicht trifft eine Verfahrenspartei insbesondere dort, wo ein Sachverhalt nur im Zusammenwirken mit der Partei oder etwa durch Vorlage von im Besitz der Partei befindlichen Beweismitteln geklärt werden kann (vgl. VwGH 15.09.2004, 2002/09/0200)."*

Im Ergebnis wurde der Beschwerde vom BVwG daher Folge gegeben und der Spruch des angefochtenen Bescheids insofern abgeändert, dass die Datenschutzbeschwerde als unbegründet abgewiesen wird.

Das Erkenntnis ist rechtskräftig.

6. Erkenntnis vom 27.Dezember.2024, W258 2227269-1/39E
Verwaltungsstrafverfahren gegen die Österreichische Post AG wegen unrechtmäßiger Verarbeitung von „Parteiaffinitäten"

Die DSB leitete aufgrund medialer Berichterstattung über den Verkauf personenbezogener Daten, insbesondere Informationen über die „politische Affinitäten" von zahlreichen betroffenen Personen, ein Ermittlungsverfahren gegen die Österreichische Post AG („ÖPAG") ein und sprach unter anderem mit Straferkenntnis vom 23. Oktober 2019 ihre bis dato höchste Geldbuße nach Art. 83 DSGVO in der Höhe von insgesamt EUR 18 Millionen aus, weil mehrere Verstöße gegen die DSGVO festgestellt werden konnten. Im Mittelpunkt stand jedoch die unrechtmäßige Verarbeitung sensibler Daten im Sinne des Art. 9 Abs. 1 DSGVO über die vermeintliche politische Meinung („Parteiaffinitäten") von mehreren Millionen Personen im gesamten Bundesgebiet Österreichs. Die Verarbeitung erfolgte im Rahmen der Ausübung des Gewerbes „Adressverlage und Direktmarketingunternehmen" und ohne Einwilligung der betroffenen Personen. Es handelte sich dabei um eine Information über die Wahrscheinlichkeit, mit der sich eine natürliche Person für Wahlwerbung einer bestimmten politischen Partei in Österreich interessiert. Eine

solche Parteiaffinität wurde jeder Person innerhalb der hierfür verwendeten Datenbank zugeordnet (rund 2,2 Millionen Personen), gespeichert und letztendlich verkauft, um es Dritten (politische Parteien) zu ermöglichen, Streuverluste in der Werbung zu reduzieren.

Die ÖPAG brachte dagegen eine Beschwerde ein und das Straferkenntnis wurde im ersten Rechtsgang vom BVwG mit Erkenntnis vom 26. November 2020, W258 2227269-1/14E, aufgrund einer damals rezenten Judikatur des VwGH im Zusammenhang mit der Strafbarkeit juristischer Personen[27] aufgehoben und das Verfahren eingestellt. Dabei wurde ins Treffen geführt, dass die DSB keine natürliche (Führungs-)Person namentlich im Spruch der Entscheidung genannt habe, die letztendlich die festgestellten Verwaltungsübertretungen zu verantworten hat. Nach Ansicht des VwGH müsse jedoch für die Strafbarkeit einer juristischen Person ein tatbestandsmäßiges, rechtswidriges und schuldhaftes Verhalten einer natürlichen Person im Spruch des Strafbescheides dargelegt und der juristischen Person zugerechnet werden.

Die DSB brachte gegen diese Entscheidung des BVwG eine außerordentliche Revision beim VwGH ein und führte unter anderem ins Treffen, dass die DSGVO eine solche Voraussetzung für die Verhängung einer Geldbuße nach Art. 83 DSGVO nicht verlange. In der Zwischenzeit initiierte das Kammergericht Berlin im Zusammenhang mit einer Geldbuße einer deutschen Aufsichtsbehörde ein Vorabentscheidungsverfahren beim EuGH, um zu prüfen, ob eine solche Zurechnung als Bedingung für die Verhängung einer Sanktion nach Art. 83 DSGVO von den Mitgliedstaaten vorgegeben werden darf oder die Voraussetzungen für die Strafbarkeit einer juristischen Person abschließend durch die DSGVO geregelt sind (in Deutschland gab es einen ähnlich gelagerten Fall in Bezug auf die Notwendigkeit einer „Zurechnungsperson"). Der VwGH setzte daraufhin das Revisionsverfahren bis zur Entscheidung des EuGH aus.[28]

Mit seinem wegweisenden Urteil vom 05. Dezember 2023[29] stellte der EuGH zusammengefasst fest, dass die materiellen Voraussetzungen für die Strafbarkeit einer juristischen Person abschließend und genau in Art. 83 DSGVO geregelt sind und einer nationalen Regelung entgegenstehen, wenn eine Geldbuße nur dann verhängt werden kann, wenn der Verstoß gegen eine Bestimmung der DSGVO zuvor einer identifizierten natürlichen Person zugerechnet wurde.

In Reaktion auf dieses Urteil änderte der VwGH seine Rechtsprechung, um der Rechtsansicht des EuGH in diesem Zusammenhang Rechnung zu tragen und hob wiederum das von der DSB angefochtene Erkenntnis des BVwG wegen Rechtswidrigkeit des Inhaltes auf. Die Beschwerde der ÖPAG gegen das Straferkenntnis musste nun vom BVwG erneut behandelt werden.

Im zweiten Rechtsgang wurde schließlich nach Durchführung von zwei mündlichen Verhandlungen zu Recht erkannt, dass im Wesentlichen der Schuldspruch im Straferkenntnis wegen der unrechtmäßigen Verarbeitung der Parteiaffinitäten bestätigt, jedoch die Geldstrafe von EUR 18 Millionen auf EUR 16 Millionen herabgesetzt wird. Das BVwG bestätigte unter anderem, dass die ÖPAG schuldhaft die (vorgeworfene) Verwaltungsübertretung nach Art. 5 Abs. 1 lit. a iVm Art. 9 Abs. 1 iVm Art. 83 Abs. 5 lit. a DSGVO zu verantworten hat. Ihr Argument, sie habe den Verstoß bzw. die rechtliche Beurteilung, dass es sich bei den genannten Informationen um personenbezogene Daten nach Art. 4 Z 1 DSGVO handeln würde, nicht erkennen können und habe daher nicht schuldhaft gehandelt, wurde vom BVwG verworfen und im Gegenteil grob fahrlässiges Verhalten festgestellt, weil sie ihre Erkundigungspflicht nicht erfüllt habe.

27 Vgl. VwGH 12.05.2020, Ro 2019/04/0229.
28 Vgl. VwGH 24.02.2022, Ra 2020/04/0187.
29 Vgl. EuGH 05.12.2023, C-807/21, Rs „Deutsche Wohnen SE".

Die von der DSB ausgesprochene Geldbuße wurde im Wesentlichen deshalb reduziert, weil im Laufe des Rechtsmittelverfahrens weitere Milderungsgründe hinzugetreten sind, indem in der Zwischenzeit (bis zum zweiten Rechtsgang) mittlerweile mehreren betroffenen Personen eine Schadenersatz-Zahlung als Vergleich angeboten und ausgezahlt sowie Unterlassungserklärungen auf Anfrage hin akzeptiert wurden. Auch die Verfahrensdauer durch einen zweiten Rechtsgang und Aussetzung bis zur Entscheidung des EuGH wurde zusätzlich mildernd berücksichtigt.

In Bezug auf die Schwere des Verstoßes war das BVwG jedoch ebenfalls der Ansicht, dass aufgrund der näher festgestellten Umstände ein hoher Schweregrad vorliegt und dem Verstoß mit einer dementsprechenden Sanktion begegnet werden muss, um die Durchsetzung der DSGVO sicherzustellen. Das BVwG hat in Folge im eigenen Ermessen eine neue Strafzumessung vorgenommen und die Geldstrafe mit EUR 16 Millionen als tat- und schuldangemessen zum Zeitpunkt der Entscheidung des Gerichts angenommen.

Die Revision wurde zugelassen. Die ÖPAG hat mittlerweile Revision an den VwGH und Beschwerde an den VfGH erhoben.

4.2.7 Verfahren über die Meldung der Verletzung des Schutzes personenbezogener Daten

Hintergrund der Regelung des **Art. 33 DSGVO** ist, dass eine Verletzung des Schutzes personenbezogener Daten einen Schaden für natürliche Personen nach sich ziehen kann, sofern keine rechtzeitige und angemessene Reaktion erfolgt. Aus diesem Grund trifft die:den Verantwortliche:n 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.

Im Berichtsjahr wurden der DSB entsprechend A**rt. 33 DSGVO 1216 nationale Sicherheitsverletzungen** („**Data Breaches**“) **gemeldet**.

Dazu kamen **39 Meldungen betreffend grenzüberschreitende Sicherheitsverletzungen** sowie 9 Sicherheitsverletzungen, die an andere Aufsichtsbehörden im Unionsgebiet herangetragen und der DSB aufgrund von potentieller Betroffenheit iSd **Art. 4 Abs. 22 DSGVO** zur Kenntnis gebracht wurden.

Von Betreiber:innen öffentlicher Kommunikationsdienste wurden **55 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:die Betreiber:in öffentlicher Kommunikationsdienste unverzüglich die DSB von dieser Verletzung zu benachrichtigen.

Auch im Jahr 2024 stand eine Vielzahl der gemeldeten Vorfälle in Verbindung mit unterschiedlichsten Arten von **Ransomware**. Ziel dürfte bei diesen Angriffen zumeist eine **Verschlüsselung von Daten** gewesen sein, je nach benutzter Software kam es mitunter auch zur Übermittlung der Daten an die Angreifer:innen. In den meisten solcher Fälle reicht dem:der Angreifer:in jedoch eine Verschlüsselung der Daten aus, um diese **gegen eine geldwerte Gegenleistung wieder zu entschlüsseln**, ohne dass eine Übertragung bzw. ein Abfluss der Daten stattfinden. Auch kam es zu einer Vielzahl von Ransomware Angriffen, bei denen von Dritten identifizierte Schwachstellen bei im Internet angebotenen Dienstleistungen ausgenutzt worden sind.

Weitere häufig gemeldete Fälle betrafen eine **Übertragung von Schadsoftware auf das System des Verantwortlichen durch das Öffnen von E-Mail-Anlagen**, wodurch in weiterer Folge E-Mails (zum Teil mitsamt dem vorherigen Schriftverkehr mit dem jeweiligen Verantwortlichen) an gespeicherte bzw. zuvor verwendete E-Mail-Adressen weitergeleitet werden.

Zudem häuften sich im Berichtsjahr Meldungen über Sicherheitsverletzungen, die Zugriffsmöglichkeiten innerhalb diverser Datenbanken durch unberechtigte Nutzer:innen auf den Bereich eines:einer berechtigten Nutzers:in betrafen.

In all den oben genannten Fällen hat die:der Verantwortliche **schnellstmöglich Maßnahmen** zu ergreifen, die **zur Reduzierung des Risikos** führen. Dazu zählen bspw. das Herunterfahren der mit Schadsoftware kompromittierten Server, das Löschen der Schadsoftware, die Abänderung der Passwörter, das Heranziehen eines:einer IT-Forensikers:in sowie die genaue Analyse bzw. Auswertung, wie es zu diesem Vorfall kommen konnte und wodurch derartige Vorfälle in Zukunft vermieden werden können.

Liegt bei einer Verletzung des Schutzes personenbezogener Daten **voraussichtlich ein hohes Risiko für die betroffenen Personen** vor, hat eine:ein Verantwortliche:r neben einer **Meldung an die DSB auch unverzüglich die betroffenen Personen zu informieren** (vgl. **Art. 34 Abs. 1 DSGVO**). Sollte eine solche Benachrichtigung unterbleiben, kann die DSB eine:einen Verantwortliche:n entsprechend **Art 58 Abs. 2 lit. e DSGVO** anweisen, eine solche Benachrichtigung nachzuholen und bei Gefahr im Verzug einen Mandatsbescheid iSd **§ 22 Abs. 4 DSG** erlassen.

Für die Einbringung von Meldungen nach **Art. 33 DSGVO** stellt die DSB auf ihrer Webseite nunmehr auch, zusätzlich zum bisherigen **PDF-Formular**, ein **Onlineformular** zur Verfügung.

Dieses ist zu finden unter https://www.formularservice.gv.at/site/fsrv/user/formular.aspx?pid=5a37966ab26c4489adc20dc53162fa4d&pn=B772da0039dbe4b5cb3db81d7171d2b2d.

4.2.8 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:die 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 Datenschutzaufsichtsbehörde verschiedene Befugnisse. Sie kann etwa dem:der Verantwortlichen bzw. Auftragsverarbeiter:in **schriftliche Empfehlungen** unterbreiten, sofern sie der Ansicht ist, dass die geplante Verarbeitung nicht im Einklang mit der DSGVO steht, etwa, weil der:die Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat. Darüber hinaus kann die Datenschutzaufsichtsbehörde sämtliche in **Art. 58 DSGVO** genannten Befugnisse ausüben.

Im Jahr 2023 wurde die DSB als Aufsichtsbehörde im Dezember 2023 in einem Fall gemäß Art. 36 DSGVO konsultiert, welcher im Jänner 2024 abgeschlossen wurde.

Im Verfahren zur **GZ: D165.007** konsultierte eine österreichische Stadt die DSB, da sie aufgrund der durchgeführten Datenschutz-Folgenabschätzung von einem hohen Risiko für Betroffene ausging. Es seien von einem privatwirtschaftlichen Unternehmen 360°-Visulisierungen von Straßen als Panoramabilder des städtischen Straßennetzes geliefert worden, welche aus einer Kamerabefahrung der gegenständlichen Stadt stammten. Zweck der Verarbeitung dieser Panoramabilder durch die Gebietskörperschaft sei die Schaffung einer Geodateninfrastruktur für Umweltpolitik, örtliche Raumplanung und Verwaltung von Verkehrsflächen. Die Gesamtbevölkerung der Stadt sei durch diese Panoramabilder des Straßennetzes betroffen, da diese auf den Aufnahmen sichtbar bzw. identifizierbar sein könnten.

Die DSB hat im Jänner 2024 den Antrag auf vorherige Konsultation nach **Art. 36 DSGVO** abgewiesen. Es wurde unter anderem verabsäumt, eine klare Abgrenzung der datenschutzrechtlichen Verantwortlichkeit hinsichtlich der potenziellen Risiken vorzunehmen. Weiters wurden ausschließlich diejenigen Datenverarbeitungsvorgänge dem Risikofaktor „hoch“ zugeordnet, welche allesamt nicht unter die datenschutzrechtliche Verantwortlichkeit der Antragstellerin fallen. Auch ist das Konsultationsverfahren nicht zur Beantwortung allgemeiner Fragestellungen hinsichtlich der Zulässigkeit von Verarbeitungstätigkeiten sowie zur Beurteilung der Angemessenheit allfälliger Zusatzangebote (bzw. der damit verbundenen Kosten) geeignet.

4.2.9 Anträge auf Genehmigung von Verhaltensregeln und Zertifizierungskriterien

4.2.9.1 Verhaltensregeln

Verhaltensregeln stellen **Leitlinien einer guten Datenschutzpraxis** dar und können die datenschutzrechtliche Verhaltensweise von Verantwortlichen und Auftragsverarbeiter:innen 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 GewO 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 **Übersicht** findet sich auf der **Website der DSB**.[30] Darüber hinaus hat auch der **EDSA Register** von Verhaltensregeln aller Mitgliedstaaten veröffentlicht, welches laufend ergänzt wird.[31]

Auf der Website der DSB findet sich auch ein *„Frage und Antworten"*-Bereich zum Thema „Verhaltensregeln und Überwachungsstellen".

4.2.9.2 Zertifizierungskriterien

Verantwortliche oder Auftragsverarbeiter:innen können von akkreditierten Zertifizierungsstellen die Erteilung einer **datenschutzrechtlichen Zertifizierung** gemäß A**rt. 42 DSGVO** beantragen. In Österreich erteilt die DSB selbst keine Zertifizierungen, sondern **akkreditiert Zertifizierungsstellen mit Bescheid**. Eine Zertifizierung durch Zertifizierungsstellen erfolgt u.a. auf Grundlage von gemäß **Art. 42 Abs. 5 DSGVO** genehmigten Zertifizierungskriterien.

Gemäß **Art. 42 DSGVO** können datenschutzspezifische Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden (Zertifizierungen). Adressat:in einer solchen Zertifizierung ist stets eine:ein Verantwortliche:r oder ein:eine Auftragsverarbeiter:in. Diese können eine Zertifizierung bei einer hierfür von der DSB **akkreditierten Zertifizierungsstelle** beantragen.

Datenschutzrechtliche Zertifizierungen sind, genauso wie branchenspezifische Verhaltensregeln gemäß **Art. 40 DSGVO**, ein **Compliance-Instrument**. Laut **ErwGr. 100 der DSGVO** sollen durch Zertifizierungen die Transparenz im Zusammenhang mit der Verarbeitung personenbezogener Daten erhöht und die Einhaltung der DSGVO verbessert werden.

Insbesondere können Zertifizierungen gemäß **Art. 42 DSGVO**

- als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten der:des Verantwortlichen nachzuweisen (Art. 24 Abs. 3 DSGVO)
- als Faktor herangezogen werden, um die Erfüllung der gemäß Art. 32 Abs. 1 DSGVO zu implementierenden technischen und organisatorischen Maßnahmen nachzuweisen (Art. 32 Abs. 3 DSGVO)
- unter den Voraussetzungen von Art. 42 Abs. 2 und 46 Abs. 2 lit. f DSGVO „geeignete Garantien" für die Übermittlung von personenbezogenen Daten an ein Drittland oder eine internationale Organisation sein
- bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag je nach Einzelfall gebührend berücksichtigt werden (Art. 83 Abs. 2 lit. j DSGVO)

30 https://dsb.gv.at/ueber-die-datenschutzbehoerde/verhaltensregeln.
31 https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en.

Gegenstand einer Zertifizierung sind gemäß **Art. 42 Abs. 1 DSGVO** allerdings immer **Verarbeitungsvorgänge im Zusammenhang mit personenbezogenen Daten**. Nach dem Konzept der DSGVO können daher bspw. Produkte von Softwarehersteller:innen, ohne einen damit in Verbindung stehenden Verarbeitungsvorgang, nicht unmittelbar gemäß A**rt. 42 DSGVO** zertifiziert werden.

Die DSB hat mit Bescheid vom 27. August 2024, **GZ: 2024-0.585.594,** erstmals (nationale) datenschutzrechtliche **Zertifizierungskriterien** gemäß **Art. 42 Abs. 5 DSGVO genehmigt**. Die Zertifizierungskriterien ermöglichen eine Zertifizierung von datenschutzrechtlichen Verantwortlichen. Folglich konnte die Zertifizierungsstelle (**DSGVO-ZT GmbH**), die breits am 21. Februar 2023 (unter aufschiebender Bedingung) akkreditiert wurde, ihre Tätigkeit aufnehmen.[32]

4.2.10 Verwaltungsstrafverfahren

Die DSB ist nach **§ 22 Abs. 5 DSG** als nationale Aufsichtsbehörde für die V**erhängung 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. Diese Aufgabe wird innerhalb der DSB von der **Abteilung V** wahrgenommen.

Die DSB hat im Berichtszeitraum im Rahmen von Verwaltungsstrafverfahren insgesamt **73 Bescheide** erlassen, davon **62** in Form von **Geldbußen** mit einer Gesamtsumme von **EUR 1.684.230,-**. 152 Verfahren wurden zur Einstellung gebracht.

Das Jahr 2024 war darüber hinaus durch zahlreiche Erkenntnisse des BVwG in datenschutzrechtlichen Verwaltungsstrafsachen geprägt. Nachdem der EuGH in der Vorabentscheidungssache **C-807/21** (*„Deutsche Wohnen SE“*) mit Urteil vom 5. Dezember 2023 wesentliche Auslegungsfragen in Bezug auf **Art. 83 DSGVO** geklärt hatte (näheres hierzu siehe Datenschutzbericht 2023, Punkt 4.2.12) und der VwGH mit Erkenntnis vom 1. Februar 2024, **Ra 2020/04/0187**, festhielt, dass unter Berücksichtigung des zitierten Urteils vom EuGH die nationalen Regelungen für die Strafbarkeit juristischer Personen gemäß **§ 30 Abs. 1 und 2 DSG** nicht zur Anwendung gebracht werden dürfen, hat das BVwG mehrere bis dahin ausgesetzte Verwaltungsstrafverfahren fortgesetzt und dabei wegweisende Entscheidungen in Bezug auf Sanktionen nach **Art. 83 DSGVO** gefällt.

Das BVwG hat im Jahr 2024 die höchsten von der DSB je verhängten Geldbußen einer Behandlung zugeführt und die Strafbarkeit juristischer Personen ausschließlich nach **Art. 83 DSGVO** beleuchtet. Hierfür waren in den jeweiligen Verfahren mehrere mündliche Verhandlungen notwendig. Die DSB war daher im Berichtszeitraum auch insbesondere damit beschäftigt, ihre wesentlichsten Straferkenntnisse der letzten Jahre vor dem BVwG zu verteidigen. In diesem Zusammenhang wird auf **Kapitel 4.2.6** des vorliegenden Datenschutzberichtes verwiesen, wo vereinzelte Erkenntnisse des BVwG in Verwaltungsstrafsachen hervorgehoben werden.

Die DSB hebt ausgewählte Entscheidungen bzw. Strafbescheide im Berichtszeitraum hervor:

32 https://dsb.gv.at/ueber-die-datenschutzbehoerde/zertifizierungen.

1. Straferkenntnis vom 2. Jänner 2024, GZ: D550.480 (OZ: 2023-0.849.065)
Verstoß gegen die Mitwirkungspflicht im Rahmen von Beschwerdeverfahren sowie Nichtbefolgung einer Anweisung der DSB

Die DSB verhängte zu Beginn des Jahres gegen ein in Österreich tätiges Medienunternehmen wegen sechs Verwaltungsübertretungen eine Geldbuße nach Art. 83 Abs. 4 und 6 DSGVO in Höhe von insgesamt EUR 15.200,-. Die Beschuldigte hatte es in insgesamt fünf Fällen verabsäumt, im Zuge eines Beschwerdeverfahrens nach Art. 77 DSGVO iVm § 24 DSG als Verantwortliche bzw. Beschwerdegegnerin mit der DSB - auf ihre mehrfachen Anfragen hin - zusammenzuarbeiten. Konkret hatte die DSB im Laufe der Beschwerdeverfahren die Beschuldigte mehrmals über verschiedene Kanäle (Mail, RSb, E-Zustellung) zu einer Stellungnahme aufgefordert. Teilweise langte auch eine Stellungnahme ein, auf die darauffolgende ergänzende Aufforderung zur Stellungnahme folgte jedoch wiederum keinerlei Reaktion. Im Rahmen der Aufforderungsschreiben wurde ausdrücklich auf die Pflicht zur Zusammenarbeit mit der Behörde hingewiesen sowie darauf, dass im Falle mangelnder Mitwirkung ein Verwaltungsstrafverfahren eingeleitet werde. Indem die Beschuldigte auf die Aufforderungen zur Stellungnahme nicht reagiert hat, stellte die DSB eine mehrfache Verletzung von Art. 31 DSGVO fest. Es handelt sich hierbei um eine strafbewehrte Verpflichtung (Art. 83 Abs. 4 lit. a DSGVO) für Verantwortliche und Auftragsverarbeiter, um mit der DSB bei der Erfüllung ihrer Aufgaben zu kooperieren.

Die DSB war mangels der Bereitschaft zur Zusammenarbeit gezwungen, die Beschwerden ohne Mitwirkung der Verantwortlichen zu erledigen, um eine allfällige Säumnisbeschwerde zu vermeiden. In einem der Beschwerdeverfahren wurde die Beschuldigte jedoch auch mittels Bescheid zur Erteilung einer Auskunft angewiesen. Der Bescheid erwuchs mangels Rechtsmittel in Rechtskraft und die betroffene Person teilte der Behörde mit, dass sie auch nach Ablauf der vordefinierten Frist noch keine Auskunft erhielt. Nach Einleitung des Verwaltungsstrafverfahrens erteilte die Verantwortliche dann die zuvor angewiesene Auskunft. Dennoch wurde im Ergebnis als Verwaltungsübertretung festgestellt, dass die Anweisung der Behörde nicht befolgt wurde, indem die Auskunft nicht innerhalb der festgelegten Frist ergangen ist. Auch die (rechtzeitige) Befolgung einer Anweisung stellt eine strafbewehrte Verpflichtung für Verantwortliche dar (Art. 83 Abs. 6 DSGVO).

Die Beschuldigte erhob eine Beschwerde gegen das Straferkenntnis vor dem BVwG. Das Verfahren ist derzeit noch anhängig.

Das BVwG hat jedoch die Strafbarkeit wegen Art. 31 DSGVO aufgrund mangelnder Mitwirkung in einem Beschwerdeverfahren schon mehrfach bestätigt (vgl. BVwG 6. Dezember 2024, W292 2285487-1; 17. September 2024, W298 2295130-1; 6. Mai 2024, W108 2281246-1; 23. Jänner 2025, W605 2284399-1). Auch die in Folge erhobene Beschwerde an den VfGH führte in zumindest zwei Fällen zu keinem Erfolg. Die Behandlung der Beschwerden wurden mittels Beschluss gemäß Art. 144 Abs. 2 B-VG abgelehnt (vgl. VfGH 16. September 2024, E 2427/2024-7; 25. November 2024, E 4123/2024-5).

2. Straferkenntnis vom 6. Juni 2024, GZ: D550.672 (OZ: 2024-0.005.787)
Sicherheitsverletzung sowie mehrere Verstöße gegen die DSGVO durch ein Covid-19-Testlabor

Die DSB hatte aufgrund medialer Berichterstattung Kenntnis über eine Sicherheitsverletzung in Bezug auf ein Unternehmen, das mit der Durchführung sowie Auswertung von Covid-19-Tests während der Pandemie beauftragt war, erlangt. Die Sicherheitsverletzung wurde nach der Berichterstattung auch unmittelbar durch das Unternehmen der DSB gemäß Art. 33 DSGVO ge-

meldet. Daraufhin wurde ein amtswegiges Prüfverfahren eingeleitet, um die technischen und organisatorischen Maßnahmen im Unternehmen zu beleuchten. Dies insbesondere in Bezug auf die E-Mail-Postfächer, da offenbar ein unbefugter Zugriff auf eines der Postfächer erfolgte und dabei eine E-Mail samt Anhang (drei Excel-Listen mit umfangreichen Gesundheitsdaten von Patienten des Testlabors) von einer unbekannten Person abgegriffen werden konnte. Innerhalb dieser (unverschlüsselten) Excel-Listen befanden sich rund 24.000 Datensätze über positive Covid-19-Testergebnisse. Die Patientendaten enthielten folgende Informationen: Vorname, Nachname, Alter, Geburtsdatum, Postleitzahl, Ort, *„Point of Care"*, Details zu den Tests wie Mutationen, Testdatum und CT-Wert. Der Versand dieser E-Mail-Nachricht erfolgte über ein der Beschuldigten zurechenbares Postfach durch einen leitenden Angestellten.

Im Laufe des Ermittlungsverfahrens zeigte die Verantwortliche kaum Bereitschaft, mit der DSB zusammenzuarbeiten, um den Sachverhalt feststellen zu können. Dennoch konnte sich die DSB einen Überblick über die vor der Sicherheitsverletzung implementierten technischen und organisatorischen Maßnahmen verschaffen und musste feststellen, dass das Postfach des leitenden Angestellten, in welchem sich auch die oben genannte E-Mail an eine externe Person befand, nicht ausreichend geschützt war. Im Hinblick darauf, dass über dieses Postfach regelmäßig bzw. täglich sensible Daten in Form von Gesundheitsdaten verarbeitet wurden, war das Postfach zwar durch ein Passwort, jedoch nicht mittels einer Zwei-Faktor-Authentifizierung vor unbefugte Zugriffe gesichert. Auch die in Verwendung gezogenen Excel-Listen mit umfangreichen Patientendaten waren durch keinerlei Maßnahmen auf Dateiebene geschützt. Es wurde somit im Ergebnis ein Verstoß gegen Art. 5 Abs. 1 lit. f iVm 32 DSGVO festgestellt.

Darüber hinaus wurden zahlreiche weitere Verstöße im Zuge der amtswegigen Prüfung festgestellt: (1) es erfolgte eine unrechtmäßige Verarbeitung sensibler Daten, indem festgestellt wurde, dass die oben genannte Mail samt Patientendaten an die externe Person gar nicht erforderlich war, (2) Verstoß gegen die Pflicht zur Benachrichtigung der Betroffenen nach Art. 34 DSGVO, weil sich die Beschuldigte weigerte, die Betroffenen über die Sicherheitsverletzung zu informieren, (3) die Archivierung der (Gesundheits-)Daten erfolgte teilweise ab einem bestimmten Zeitpunkt über einen Auftragsverarbeiter, jedoch wurde kein schriftlicher Auftragsverarbeitungsvertrag abgeschlossen (die ins Treffen geführte mündliche Vereinbarung wurde nicht akzeptiert), (4) es wurde keine geeignete Datenschutzbeauftrage benannt, weil festgestellt werden musste, dass die vom Unternehmen bestellte Datenschutzbeauftragte kein Fachwissen oder berufliche Qualifikationen auf dem Gebiet des Datenschutzrechts zum Zeitpunkt ihrer Bestellung hatte und demnach auch nicht die Fähigkeit, die in Art. 39 DSGVO genannten Aufgaben zu erfüllen. Es konnte keine geeignete Praxiserfahrung oder abgeschlossene Ausbildungen vorgewiesen werden, (5) der DSB wurde die Bestellung der Datenschutzbeauftragten gar nicht gemeldet, sondern erst mit der Meldung der Sicherheitsverletzung.

Obwohl der Betrieb des Labors zum Zeitpunkt des Straferkenntnisses bereits eingestellt war, verhängte die DSB aufgrund der oben festgestellten Verstöße eine Sanktion in Höhe von insgesamt EUR 100.000,-. Dagegen wurde eine Beschwerde eingebracht.

Das Verfahren ist derzeit beim BVwG anhängig.

3. Straferkenntnis vom 16. August 2024, GZ: D550.761 (OZ: 2023-0.680.196) Unrechtmäßige Verarbeitung durch Betrieb einer Videoüberwachungsanlage

Die höchste im Berichtszeitraum von der DSB verhängte Geldbuße betraf den unrechtmäßigen Betrieb einer Videoüberwachungsanlage (bestehend aus neun Außen- und Innenkameras) in einem stark von Fußgänger:innen frequentierten Bereich innerhalb von Wien betrieben. Die

Geldbuße wurde dabei gegenüber einer juristischen Person, die einem Unternehmen im Sinne des Art. 101 und 102 AEUV (d.h. einem Konzern) angehört, ausgesprochen. Die DSB orientierte sich dabei an der Entscheidung des EuGH in Bezug auf die Strafbarkeit juristischer Personen. Der EuGH stellte in einer wegweisenden Entscheidung unter anderem fest, dass Aufsichtsbehörden bei der Berechnung einer Geldbuße nach Art. 83 DSGVO verpflichtet sind, den Begriff „Unternehmen" im Sinne der Art. 101 und 102 AEUV auszulegen, wenn die Verantwortliche einer sogenannten wirtschaftlichen Einheit, die auch aus mehreren juristischen Personen bestehen kann, angehört. Nur dadurch kann letztlich sichergestellt werden, dass eine Geldbuße, deren Höhe anhand der tatsächlichen Leistungsfähigkeit des Adressaten festgesetzt wird, die drei in Art. 83 Abs. 1 DSGVO zentralen Voraussetzungen einer Geldbuße (wirksam, abschreckend und verhältnismäßig) erfüllt (vgl. EuGH 5. Dezember 2023, Rn 56 bis 59).

Die DSB brachte bei der Strafzumessung die Leitlinien des EDSA zur Berechnung von Geldbußen nach Art. 83 DSGVO zur Anwendung (vgl. Leitlinien 04/2022, Version 2.1, angenommen am 24.05.2023). Durch diese Leitlinien soll sichergestellt werden, dass durch Aufsichtsbehörden einheitliche Sanktionen verhängt werden.[33] In Bezug auf die Strafzumessung wird auch durch die Leitlinien vorgegeben, dass die Unternehmensgröße als ein wesentlicher Faktor herangezogen wird. Die DSB hat im vorliegenden Fall zwar die überdurchschnittliche Unternehmensgröße (mehr als EUR 500 Mio. Jahresumsatz) berücksichtigt, aber auch insbesondere auf die Verhältnismäßigkeit geachtet.

Im Ergebnis wurde daher unter Anwendung der Kriterien nach Art. 83 Abs. 1 und 2 DSGVO und Berücksichtigung der Unternehmensgröße beschlossen, eine Geldbuße in Höhe von EUR 1.500.000,- auszusprechen. Die Verantwortliche erhob dagegen eine Beschwerde.

Das Verfahren ist derzeit beim BVwG anhängig.

4. Straferkenntnis vom 16. Oktober 2024, GZ: D550.769 (OZ: 2024-0.641.771)
Interessenskonflikt beim Datenschutzbeauftragten

Die Beschuldigte hatte über einen Zeitraum von drei Jahren ihren handelsrechtlichen Geschäftsführer, welcher überdies Gesellschafter war, gleichzeitig als Datenschutzbeauftragten benannt. Die benannte Person war aufgrund ihrer Doppel- bzw. Dreifachrolle jedenfalls nicht als eine von der Beschuldigten unabhängige Stelle zu qualifizieren, welche die Aufgabe der Überwachung der Einhaltung der DSGVO sowie der Strategien des:der Verantwortlichen oder des:der Auftragsverarbeiters:in für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter:innen und der diesbezüglichen Überprüfungen vornehmen konnte. Dadurch war eine von der Geschäftsführung vorzunehmende unabhängige Kontrolle durch den Datenschutzbeauftragten ausgeschlossen. Vielmehr lag eine Art der Selbstkontrolle vor, welche keiner unabhängigen objektiven Überprüfung eines:einer Dritten zugänglich war. Die Beschuldigte hat dadurch im Ergebnis eine nicht geeignete Person als Datenschutzbeauftragten benannt und musste einen Verstoß gegen Art. 38 Abs. 6 DSGVO verantworten, dem mit einer Geldbuße in Höhe von EUR 5.000,- begegnet wurde.

Das Straferkenntnis ist rechtskräftig.

33 Die Leitlinien des EDSA zur Strafbemessung wurden in rezenten Entscheidungen des Bundesverwaltungsgerichts ebenfalls zur Anwendung gebracht, um eine einheitliche Methode für die Strafbemessung sicherzustellen: z.B. BVwG 27.03.2024, W214 2243436-1; 07.06.2024, W256 2246230-1.

4.2.11 Stellungnahmen zu Gesetzes- und Verordnungsentwürfen

Die DSB hat im Jahr 2024 zu folgenden Vorhaben eine **Stellungnahme** abgegeben:

1. Zweite Transparenzdatenbank-Abfrageverordnung 2023
2. Bundesgesetz, mit dem das Denkmalschutzgesetz geändert wird
3. VersSt-Informationspflichtenverordnung 2023
4. Landesgesetz, mit dem das Wiener Tanzschulgesetz 1996 geändert wird
5. Berufsrechts-Änderungsgesetz 2024
6. Schulordnung 2024
7. Tierschutzgesetz
8. Bundesgesetz, mit dem das Einkommensteuergesetz 1988 und das Gebührengesetz 1957 geändert werden
9. Bundesgesetz, mit dem das KommAustria-Gesetz und das Telekommunikationsgesetz 2021 geändert werden
10. 35. StVO-Novelle
11. Elektrizitätswirtschaftsgesetz, Energiearmuts-Definitions-Gesetz sowie Änderung Energie-Control-Gesetz
12. Bundesgesetz, mit dem das Psychotherapiegesetz 2024 – PthG 2024 erlassen sowie das Musiktherapiegesetz, das Psychologengesetz 2013 und das Universitätsgesetz 2002 geändert werden
13. Landesgesetz, mit dem das Wiener Mindestsicherungsgesetz (WMG) geändert wird
14. Bundesgesetz, mit dem das Druckgerätegesetz geändert und das Gesetz in Bezug auf die Emissionsgrenzwerte für gasförmige Schadstoffe und luftverunreinigende Partikel und die Typgenehmigung für Verbrennungsmotoren für nicht für den Straßenverkehr bestimmte mobile Maschinen und Geräte erlassen wird
15. Bundesgesetz, mit dem die Notariatsordnung, die Rechtsanwaltsordnung und das Disziplinarstatut für Rechtsanwälte und Rechtsanwaltsanwärter geändert werden (Berufsrechts-Änderungsgesetz 2024)
16. Novelle der Quotenregelungsverordnung
17. Novelle der GewO 1994
18. Recyclinggips-Verordnung
19. Transparenzdatenbank - Förderungsschienenverordnung
20. Novelle des Arbeitslosenversicherungsgesetzes 1977
21. Bundesgesetz, mit dem das Netz- und Informationssystemsicherheitsgesetz 2024 erlassen wird und das Telekommunikationsgesetz 2021 sowie das Gesundheitstelematikgesetz 2012 geändert werden
22. Novelle des Zivildienstgesetzes 1986
23. Cybersicherheitszertifizierungs-Gesetz
24. Landesgesetz, mit dem das Gesetz über Leistungen und Einrichtungen für altersbedingte Pflege und Betreuung (Steiermärkisches Pflege- und Betreuungsgesetz) erlassen und das Steiermärkische Sozial- und Pflegeleistungsfinanzierungsgesetz, das Steiermärkische Behindertengesetz, das Steiermärkische Sozialunterstützungsgesetz und das Steiermärkische Nächtigungsabgabegesetz geändert werden
25. Novelle der Patentamtsverordnung 2019
26. Bundesgesetz, mit dem ein Qualifizierte Einrichtungen Gesetz erlassen wird und die Zivilprozessordnung, das Konsumentenschutzgesetz, das Gerichtsgebührengesetz und das Rechtsanwaltstarifgesetz geändert werden (Verbandsklagen-Richtlinie-Umsetzungs-Novelle)
27. Bundesgesetz, mit dem das Arbeitsvertragsrechts-Anpassungsgesetz, das Arbeitsverfassungsgesetz, das Arbeitsinspektionsgesetzes 1993, das

Dienstnehmerhaftpflichtgesetz, das Allgemeine Sozialversicherungsgesetz, das Beamten-Kranken- undUnfallversicherungsgesetz, das Notarversorgungsgesetz, das Einkommensteuergesetz 1988, das Heimarbeitsgesetz und das Landarbeitsgesetz 2021 geändert werden (Telearbeitsgesetz)

28. Novelle des Sozialbetrugsbekämpfungsgesetzes (Betrugsbekämpfungsgesetz 2024 Teil II)
29. Novelle des Datenschutzgesetzes
30. Novelle des Sicherheitspolizeigesetzes
31. Novelle des Geschäftsordnungsgesetzes sowie Bundes-Verfassungsgesetzes u.a. (427/AUA)
32. Transparenzdatenbank-Abfrageverordnung 2024
33. Novelle des Bundeshaushaltsgesetzes 2013
34. Bundesgesetz, mit dem das Schulorganisationsgesetz, das Schulunterrichtsgesetz, das Schulunterrichtsgesetz für Berufstätige, Kollegs und Vorbereitungslehrgänge, das Bildungsdokumentationsgesetz 2020 und das Schulpflichtgesetz 1985 geändert werden
35. Bundesgesetz, mit dem das Gesundheits- und Krankenpflegegesetz und das Rezeptpflichtgesetz geändert werden (GuKG-Novelle 2024)
36. Strafprozessrechtsänderungsgesetz 2024
37. EAG-Investitionszuschüsseverordnung-Wasserstoff
38. Bundesgesetz über die gehobenen medizinisch-therapeutisch-diagnostischen Gesundheitsberufe (MTD-Gesetz 2024 – MTDG)
39. Landesgesetz über den Einsatz moderner Informationstechnologien zur Förderung der digitalen Transformation der Verwaltung (Oö. Informationstechnologien-Einsatz-Gesetz)
40. Landesgesetz, mit dem das Wiener Kindergartengesetz (WKGG) geändert wird
41. Landesgesetz, mit dem das Wiener Tagesbetreuungsgesetz (WTBG) geändert wird
42. Bundesgesetz, mit dem das Staatsschutz- und Nachrichtendienstgesetz (SNG) geändert wird
43. Verordnung des Bundesministers für Soziales, Gesundheit, Pflege und Konsumentenschutz über die Einrichtung und Führung der Tierärzteliste und der Liste hausapothekenführender Tierärztinnen und Tierärzte sowie über die Form und den Inhalt des Tierärzteausweises (Tierärzteliste und -ausweisVO)
44. Verordnung des Bundesministers für Soziales, Gesundheit, Pflege und Konsumentenschutz mit den Verordnungen im Zusammenhang mit dem Tierarzneimittelgesetz erlassen und weitere Verordnungen geändert werden
45. Bundesgesetz, mit dem das Bundesgesetz über Daten-Governance, Anbieter von Datenvermittlungsdiensten und datenaltruistische Organisationen nach der Verordnung (EU) 2022/868 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Datenzugangsgesetz – DZG) erlassen wird
46. Bundesgesetz, mit dem das Finanzmarkt-Geldwäschegesetz, das Wirtschaftliche Eigentümer Registergesetz, das Finanzmarktaufsichtsbehördengesetz und das Glücksspielgesetz geändert werden (FM-GwG-Anpassungsgesetz)
47. Bundesgesetz, mit dem ein Sanktionengesetz 2024 erlassen wird, das Sanktionengesetz 2024, das Bankwesengesetz, das E-Geldgesetz 2010, das Finanzmarktaufsichtsbehördengesetz, das Verbraucherzahlungskontogesetz, das Devisengesetz 2004, das Staatsschutz- und Nachrichtendienst-Gesetz und das Kontenregister- und Konteneinschaugesetz geändert werden (FATF-Prüfungsanpassungsgesetz 2024)
48. Landesgesetz, mit dem das Parkometergesetz 2006 geändert wird
49. Landesgesetz, mit dem das Wiener Mindestsicherungsgesetz (WMG) geändert wird
50. Landesgesetz, mit dem das Tiroler Freizeitwohnsitz- und Leerstandsabgabegesetz (TFLAG) geändert wird

Die Stellungnahmen sind, soweit es sich nicht um jene zu Verordnungen handelt, unter www.parlament.gv.at bzw. im Fall von Landesgesetzen auf den Webseiten der Länder/Landtage abrufbar.

5. Wesentliche höchstgerichtliche Entscheidungen

Wie jedes Jahr war auch 2024 durch eine intensive Entscheidungstätigkeit der Höchstgerichte auf (inter)nationaler Ebene geprägt.

5.1. Verfassungsgerichtshof

Dieses Jahr stechen vor allem zwei Erkenntnisse des VfGH mit Bezug zum Datenschutz heraus. So hat das Höchstgericht geklärt, dass zur Überprüfung der Rechtmäßigkeit einer Investorenwarnung nicht die DSB, sondern die FMA zuständig ist und erkannt, dass das Anti-Gesichtsverhüllungsgesetz als (auch) verfassungskonform mit dem Grundrecht auf Datenschutz zu beurteilen ist.

1. Erkenntnis vom 26. Februar 2024, E 3481/2022

In dieser den Datenschutz am Rande streifenden Entscheidung sprach der VfGH eine Verletzung im Recht auf Gleichheit aller Staatsbürger:innen vor dem Gesetz durch eine erkennungsdienstliche DNA-Untersuchung nach § 67 SPG aus, konkret durch einen unfreiwillig durchgeführten Mundhöhlenabstrich aufgrund des Verdachtes des versuchten Widerstandes gegen die Staatsgewalt (§§ 15, 269 StGB) im Rahmen einer Vernehmung.

U.a. gegen diesen Mundhöhlenabstrich richtete die Beschwerdeführerin zunächst eine Maßnahmenbeschwerde an das LVwG und anschließend gegen dessen teils abweisendes, teils zurückweisendes Erkenntnis eine Beschwerde nach Art. 144 B-VG an den VfGH. Dieser erkannte die Rechtsverletzung in den Grundrechten der Beschwerdeführerin im Zusammenhang mit § 67 SPG darin, dass das LVwG sein Erkenntnis mit Willkür belastet hat, indem es die von § 67 SPG (DNA-Untersuchungen) als lex specialis von § 65 SPG (Erkennungsdienstliche Behandlung) geforderte Gefährlichkeitsprognose unterließ, wonach eine DNA-Untersuchung nur dann zulässig ist, wenn wegen der Art oder Ausführung der Persönlichkeit des Betroffenen zu befürchten ist, er werde gefährliche Angriffe begehen und dabei Spuren hinterlassen, die seine Wiedererkennung auf Grund der ermittelten genetischen Daten iSd § 36 Abs. 2 Z 12 DSG ermöglichen würden. Da diese Prognose fehlte, war das Erkenntnis des LVwG diesbezüglich aufzuheben.

2. Erkenntnis vom 12. März 2024, E 3436/2023

Ausgangspunkt dieses Verfahrens war eine von der FMA am 2. September 2020 im Internet und in der Wiener Zeitung kundgemachte „Investorenwarnung“ gemäß § 92 Abs. 11 erster Satz WAG 2018, wonach die beschwerdeführende Partei, eine juristische Person, nicht berechtigt sei, konzessionspflichtige Wertpapierdienstleistungen in Österreich zu erbringen. Mit Bescheid vom 23. Oktober 2020 stellte die FMA fest, dass die Veröffentlichung rechtmäßig sei. Auch das BVwG wies die Beschwerde als unbegründet ab. Mit Bescheid vom 9. Juni 2021 forderte die FMA die beschwerdeführende Partei gemäß § 3 Abs. 2 Z 3 WAG 2018 weiters auf, die unerlaubte gewerbliche Anlageberatung in Bezug auf Finanzinstrumente und die unerlaubte gewerbliche Anlageberatung und Übermittlung von Aufträgen zu unterlassen. Die Bekämpfung dieses

Bescheides durch die beschwerdeführende Partei blieb ebenso erfolglos. Angesichts dessen hat die Beschwerdeführerin keine Finanzprodukte mehr angeboten und ihren Firmennamen, -gegenstand und –sitz geändert. Daraufhin hat die beschwerdeführende juristische Person einen Antrag auf Löschung an die FMA gestellt sowie einen Antrag auf Auskunft des Zwecks der Verarbeitung sowie der Speicherdauer, sollte sie nicht gewillt sein, die „Investorenwarnung" bzgl. der Beschwerdeführerin zu löschen. Nachdem die FMA dem Antrag nicht nachkam, hat die beschwerdeführende Partei am 17. November 2021 eine Beschwerde bei der DSB eingebracht. Die DSB gab dem Beschwerdebegehren bzgl. der Löschung und der Auskunft mit Bescheid vom 3. August 2022 statt, da sich durch das Entfernen des „Footers" auf der Homepage der beschwerdeführenden Partei, welche ursprünglich zu der Investorenwarnung gemäß § 92 Abs. 11 erster Satz WAG 2018 geführt wurde, eine neue Sachlage ergeben habe, aufgrund derer es erforderlich sei, die Datenverarbeitungslegitimation neu zu prüfen. Das BVwG gab einer hiergegen gerichteten Bescheidbeschwerde der FMA statt und wies die Beschwerde mit der Begründung zurück, die beschwerdeführende Partei könne als juristische Person keine Beschwerde nach § 24 DSG erheben.

Der VfGH hat die diesbezügliche Frage bei gleichzeitiger Bejahung, dass das Grundrecht auf Datenschutz nach § 1 DSG grundsätzlich auch für juristische Personen gilt, gegenständlich dahingestellt gelassen, da die DSB keinesfalls zu einer Entscheidung über Beschwerden im Zusammenhang mit Veröffentlichungen („Investorenwarnungen") gemäß § 92 Abs. 11 vierter Satz WAG 2018 zuständig ist. Hier gibt es nämlich einen eigenen administrativrechtlichen Rechtschutz(weg) an die FMA, welcher natürlichen sowie juristischen Personen offensteht. In diesem hat die FMA auch zu prüfen, ob die rechtlichen Voraussetzungen für eine „Investorenwarnung" vorliegen und in dem Zusammenhang auch eine Verletzung des Grundrechtes auf Geheimhaltung personenbezogener Daten iSd § 1 Abs. 1 DSG auszuschließen ist. Sollte für die FMA einen Verstoß gegen das Grundrecht auf Datenschutz einer natürlichen oder juristischen Person vorliegen, wäre sie gemäß § 92 Abs. 11 vierter Satz WAG 2018 gehalten, im Hinblick auf § 1 Abs. 3 DSG die Veröffentlichung richtigzustellen, zu widerrufen oder zu löschen.

Sollte sich der Sachverhalt, wie von der Beschwerdeführerin vorgebracht, seit dem Bescheid vom 23. Oktober 2023 geändert haben, ist bei der FMA die neuerliche Durchführung eines Verfahrens nach § 92 Abs. 11 vierter Satz WAG 2018 zu beantragen. Da es im gegenständliche Fall lediglich darum geht, ob die auf § 92 Abs. 11 WAG 2018 gestützte Veröffentlichung (nach wie vor) rechtmäßig ist, ist zur Beurteilung der Rechtmäßigkeit der „Investorenwarnung" ausschließlich die FMA und nicht die DSB zuständig.

3. Erkenntnis vom 3. Oktober 2024, E 4003/2023

Ein LVwG stellte in seinem Erkenntnis fest, dass der Beschwerdeführer am 19. Mai 2023 auf einem Bahnhofsplatz „seine Gesichtszüge mit einer Burka (Ganzkörperschleier mit ‚vergitterten' Sehschlitz im Augenbereich) verhüllt [hat]. Die Gesichtszüge waren nicht mehr erkennbar. Der Beschwerdeführer wollte durch die den öffentlichen Raum erfassende Videoüberwachungskamera nicht erfasst werden und in der Öffentlichkeit nicht erkannt werden." Mit Bescheid der zuständigen Bezirkshauptmannschaft vom 18. Juli 2023 wurde über die beschwerdeführende Partei eine Geldstrafe in Höhe von € 50,- bzw. im Falle der Uneinbringlichkeit eine Ersatzfreiheitsstrafe von 20 Stunden verhängt, weil er durch sein Verhalten gegen § 2 Anti-Gesichtsverhüllungsgesetz (AGesVG) verstoßen habe.

In der gegen diesen Bescheid erhobenen Beschwerde brachte der Beschwerdeführer vor, dass das AGesVG verfassungswidrig sei. Insbesondere verstoße es gegen das Grundrecht auf Datenschutz, weil die Verhüllung des Gesichtes beim Durchschreiten von öffentlichen Orten, die

videoüberwacht werden, der einzige Weg sei, einer Datenverarbeitung zu entgehen. Es müsse jedermann freistehen, zu entscheiden ob er auf das Durchschreiten solcher Orte verzichte oder sie mit verhülltem Gesicht durchquere. Das LVwG folgte der Meinung des Beschwerdeführers nicht und stellte den Sachverhalt fest wie bereits ausgeführt.

Auch der VfGH folgte dem – sich auch auf andere Grundrechte stützenden – Vorbringen der beschwerdeführenden Partei nicht, da dem Gesetzgeber zusammengefasst ein weiter Ermessensspielraum zur Förderung von Integration durch Stärkung der Teilhabe an der Gesellschaft und Sicherung des friedlichen Zusammenlebens zukommt und der VfGH weiters auch keine kompetenzrechtlichen Bedenken gegen das AGesVG hat. Der VfGH scheint in der Gesichtsverhüllung dementsprechend keinen Akt der Selbsthilfe bzgl. des Grundrechtes auf Datenschutz zu sehen bzw. kann sie nicht zur Verteidigung desselben eingesetzt werden.

5.2. Oberster Gerichtshof

1. Beschluss vom 21. Februar 2024, 6 Ob 236/23h

In dieser Sache ging es um die Frage der Gerichtszuständigkeit für eine auch auf Art. 82 DSGVO gestützte Klage gegen zwei verbundene Medienunternehmen (Unterlassung, Beseitigung/Löschung und Schadenersatz, Print und Online) wegen Datenverarbeitung für journalistische Zwecke. Diesbezüglich hielt der OGH fest, dass die Zuständigkeit des angerufenen Zivilgerichts zwar grundsätzlich gegeben ist, wenn dessen örtliche Zuständigkeit in Ansehung auch nur eines Rechtsgrundes vorliegt (hier: Gericht am Wohnort des Klägers/Betroffenen, Zuständigkeit nach § 29 Abs. 2 1. Fall DSG). Das Medienprivileg nach § 9 Abs. 1 DSG (idF vor BGBl. I Nr. 62/2024) bewirkt jedoch, dass die im Datenschutzgesetz verankerte Norm über die Zuständigkeit gemäß § 29 Abs. 2 DSG in einem Verfahren gegen eine Medieninhaberin keine Anwendung findet, soweit diese Daten zu journalistischen Zwecken verarbeitet hat. Entfällt die Anwendung des § 29 DSG, verbleibt dem Kläger für die Verfolgung seiner Ansprüche aus der Verletzung eines Persönlichkeitsrechts (also auch für Eingriffe in sein Recht auf Datenschutz, deren Berechtigung erst im Hauptverfahren zu prüfen ist) der Gerichtsstand nach § 92b JN (das Gericht, in dessen Sprengel das schädigende Ereignis eingetreten ist oder einzutreten droht), vorausgesetzt die Verletzung des Rechts auf Datenschutz als eine Verletzung eines Persönlichkeitsrechts fand in einem elektronischen Kommunikationsnetz statt.

2. Beschluss vom 15. Mai 2024, 6 Ob 70/24y

Der Kläger verlangte von einer Liegenschaftseigentümerin, gleichzeitig seine Vermieterin, gestützt auf Art. 82 DSGVO Schadenersatz, weil diese Bilddaten einer Videoüberwachung des Mieter-Parkplatzes an die Kaskoversicherung des Klägers übermittelt hatte. Diese hatte daraufhin die Deckung von Reparaturkosten am Pkw des Klägers nach einem selbstverursachten Parkschaden wegen grober Fahrlässigkeit (aus den Bilddaten hervorgehende, augenscheinlich schwere Alkoholisierung des Klägers) abgelehnt. Der Kläger verlangte nun den Ersatz der Reparaturkosten von der Liegenschaftseigentümerin mit dem Argument, ohne die nach Meinung des Klägers rechtswidrig vorgenommene Bilddatenverarbeitung hätte die Kaskoversicherung den Schaden decken müssen. Erst- und Berufungsgericht wiesen die Klage mangels Rechtswidrigkeitszusammenhangs – dieser Schadenersatzanspruch ist nicht vom Schutzzweck der datenschutzrechtlichen Bestimmungen umfasst – ab. Der OGH bestätigte dies und wies die (zugelassene, ordentliche) Revision zurück.

3. Beschluss vom 9. Juli 2024, 10 ObS 11/24a

Sozialrechtlicher Streitgegenstand war die Gewährung einer vorzeitigen Invaliditätspension (Mindestalter: 60 Jahre). Der Kläger, der aus der Türkei nach Österreich eingewandert war, hatte sein Geburtsjahr im Antrag bei der Pensionsversicherungsanstalt im Jahr 2010 mit 1965 angegeben, 2016 aber eine Gerichtsentscheidung in der Türkei erwirkt, in dem dieses auf 1958 berichtigt wurde. Erst- und Berufungsgericht wiesen die Klage ab, da gemäß § 358 Satz 1 ASVG für die Feststellung des Geburtsdatums der versicherten Person die erste schriftliche Angabe der versicherten Person gegenüber dem Versicherungsträger heranzuziehen ist. Der OGH hat die außerordentliche Revision des Klägers nicht zugelassen. Weder liegt ein offenkundiger Schreibfehler, noch eine ältere Urkunde vor, aus der ein früheres Geburtsdatum hervorgeht. Die DSGVO ist auf eine Erhebung des Geburtsdatums im Jahr 2010 nicht anzuwenden. Eine spätere, auf Art. 16 DSGVO gestützte Berichtigung des Geburtsdatums in den Datenverarbeitungen der Sozialversicherungsträger, einschließlich der E-Card, ist nicht entscheidend, da Inhalt der nach § 358 ASVG verarbeiteten Daten nicht das biologische Geburtsdatum der versicherten Person, sondern die Tatsache ist, dass sie zu einem bestimmten Zeitpunkt ein bestimmtes Datum als ihr Geburtsdatum angegeben hat. Der Kläger und Revisionswerber hat nach Ansicht des OGH auch keine Unvereinbarkeit von § 358 ASVG mit der DSGVO aufgezeigt.

Das Verfahren hat Bezug zum Bescheid der DSB vom 17. Juli 2017, GZ: DSB-D122.682/0006-DSB/2017 (nicht veröffentlicht), zum Erkenntnis des BVwG vom 4. September 2019, Zl. W101 2168337-1, und zu den Beschlüssen des VfGH vom 26. November 2020, Zl. E 3828/2019 (Ablehnung der Behandlung einer Beschwerde nach Art. 144 B-VG, keine Prüfung der Verfassungsmäßigkeit von § 358 ASVG) und vom 12. Juni 2023, Zl. G 206/2023 (Ablehnung eines Individualantrags auf Prüfung der Verfassungsmäßigkeit von § 358 ASVG), obwohl es sich nicht in allen Fällen um dieselbe Partei handelt.

4. Urteil vom 27.08.2024, 6 Ob 233/23t

Gegenstand dieser Streitsache einer betroffenen Person als Kläger gegen die Stadt Wien als Trägerin einer öffentlichen Krankenanstalt und datenschutzrechtlich Verantwortliche war das Recht auf Auskunft in Form der Kopie der Daten einer Krankengeschichte (Behandlungsdokumentation) und die Frage eines Anspruchs der Verantwortlichen auf Kostenersatz dafür. Nach einer ersten Entscheidung des OGH (Beschluss vom 17. Dezember 2020, 6 Ob 138/20t) war das Verfahren im zweiten Rechtsgang bis zum Urteil des EuGH vom 26. Oktober 2023 in der Rechtssache C-307/22 ausgesetzt worden. Im Revisionsurteil stellte der OGH die stattgebende Entscheidung des Erstgerichts inhaltlich wieder her. Der Kläger hat gemäß Art. 15 Abs. 3 und Art. 12 Abs. 5 DSGVO grundsätzlich Anspruch auf eine kostenlose erste Kopie seiner Krankengeschichte. Einschränkungen der in Art. 15 DSGVO eingeräumten Betroffenenrechte müssen den Anforderungen des Art. 23 DSGVO genügen. Im konkreten Fall erachtete der OGH die Kostenersatzpflicht nach § 17a Abs. 2 lit. g Wiener Krankenanstaltengesetz 1987 für nicht mit der DSGVO vereinbar, weshalb die Bestimmung unangewendet zu bleiben hatte.

5.3. Verwaltungsgerichtshof

Der VwGH hat dieses Jahr zahlreiche Entscheidungen getroffen, welche die Spruchpraxis der DSB in den folgenden Jahren prägen werden.

1. Erkenntnis vom 1. Februar 2024, Ra 2021/04/0088

In dieser Entscheidung erklärte der VwGH, dass auch die Tätigkeit eines Gerichtsvollziehers im Auftrag eines Bezirksgerichtes eine justizielle Tätigkeit nach Art. 55 Abs. 3 DSGVO darstellen kann. Im zugrundeliegenden Fall hatte ein Gerichtsvollzieher den Verpflichteten nicht angetroffen und daraufhin eine Visitenkarte an die Tür geheftet. Die DSB bejahte ihre Zuständigkeit in der dagegen gerichteten Beschwerde wegen der behaupteten Verletzung im Recht auf Geheimhaltung. Das BVwG hob den Bescheid ersatzlos auf, da auch diese Tätigkeit eine justizielle Tätigkeit darstellt und die DSB unzuständig sei. Der VwGH schloss sich dieser Ansicht an und verwies auf das EuGH Urteil vom 24. März 2022, C-245/20, in dem der EuGH den Begriff „justizielle Tätigkeit" weit auslegte und ausgesprochen hatte, dass auch die Weitergabe von Informationen an Medien durch Gerichte unter justizielle Tätigkeit fällt.

2. Erkenntnis vom 6. März 2024, Ro 2021/04/0027

Mit diesem revisionsabweisenden Erkenntnis hat der VwGH klargestellt, dass nicht jedenfalls eine Rechtsverletzung nach der DSGVO festgestellt werden muss. Ausgangssachverhalt für die (Bescheid)Beschwerde und anschließende ordentliche Revision war eine unvollständig erteilte Auskunft der Verantwortlichen nach Art. 15 DSGVO. Diese Auskunft wurde im Verfahren vor der DSB nachgeholt. Nach § 24 Abs. 6 DSG kann ein Beschwerdegegner bis zum Abschluss des Verfahrens vor der Datenschutzbehörde die behauptete Rechtsverletzung nachträglich beseitigen, indem er den Anträgen des Beschwerdeführers entspricht. Erscheint der DSB die Beschwerde insofern als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist er darauf aufmerksam zu machen, dass die DSB das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet.

Die DSB ging im gegenständlichen Verfahren nach § 24 Abs. 6 DSG vor. Da der Beschwerdeführer widersprach, da im gegenständlichen Verfahren vor der DSB aber keine Gründe vorhanden waren, die für eine unvollständige Auskunft gesprochen hätten, hat die DSB die Beschwerde abgewiesen. Auch das BVwG wies die Beschwerde ab. Der VwGH hat erkannt, dass die Feststellung einer Verletzung in seinen Rechten zugunsten eines Beschwerdeführers, der die Feststellung der Nichterfüllung einer datenschutzrechtlich gebotenen Leistung wie u.a der Auskunft begehrt, nicht mehr in Frage kommt, wenn der Beschwerdegegner dem Leistungsbegehren nachgekommen ist. Dem steht auch die DSGVO nicht entgegen. Deren Bestimmungen verlangen laut VwGH, der dabei auf die Auflistung der Befugnisse der Aufsichtsbehörde in Art. 58 Abs. 1 bis 3 DSGVO verweist, selbst ausdrücklich keine Feststellung einer Rechtsverletzung und geht dies auch weder aus Art. 77 DSGVO (Recht auf Beschwerde bei einer Datenschutzaufsichtsbehörde) noch aus Art. 15 DSGVO (Recht auf Auskunft) selbst hervor. Im Gegenteil obliegt die Regelung des Verfahrensrechtes im Zusammenhang mit der DSGVO den Mitgliedstaaten und verweist der VwGH dabei auf Art. 58 Abs. 4 DSGVO.

3. Erkenntnis vom 6. März 2024, Ro 2021/04/0030

Dieses Erkenntnis war thematisch ähnlich gelagert. Der VwGH stellte für das zugrundeliegende Beschwerdeverfahren, in dem es u.a. um das unzureichend beantwortete Auskunftsbegehren der Betreiberin einer Identitäts- und Bonitätsdatenbank ging sowie um eine Verletzung im Recht auf Information nach Art. 14 DSGVO, Folgendes fest: das Recht auf Erhalt von Informationen bedarf, anders als das Recht auf Auskunft, keines Antrages oder Leistungsbegehrens an den Verantwortlichen, weshalb die Verletzung von Art. 14 DSGVO auch keiner nachträglichen Beseitigung zugänglich ist. Daran ändert auch Art. 14 Abs. 5 DSGVO nichts, wonach Art. 14 Abs.

1 bis 4 DSGVO keine Anwendung findet, wenn die betroffene Person bereits über die Information verfügt. Eine solche Ausnahme kann sich nämlich nur auf den Zeitpunkt beziehen, zu dem die Informationspflicht zu erfüllen gewesen wäre.

Dasselbe dürfte auch für Art. 13 DSGVO gelten.

4. Erkenntnis vom 2. April 2024, Ro 2021/04/0008

Mit diesem Erkenntnis bekräftigt der VwGH unter Verweis auf das Urteil des EuGH zu C-634/21 (Rn. 48 und 73) sein Erkenntnis vom 21. Dezember 2023, Ro 2021/04/0010, in dem er erkannt hat, dass eine automatisierte Datenverarbeitung wie Profiling selbst eine „automatisierte Entscheidung im Einzelfall" iSd Art. 22 Abs. 1 DSGVO darstellt, wenn das Ergebnis das Handeln Dritter „maßgeblich leitet" und so den Betroffene erheblich beeinträchtigt. Weiters stellt er klar, dass der Umstand, dass der Verantwortliche das Ergebnis des Profiling (bloß) an eine dritte Person weitergibt, die darauf aufbauend eine Entscheidung trifft, nichts daran ändert, dass das Profiling selbst eine automatisierte Entscheidung iSd Art. 22 Abs. 1 DSGVO darstellt, sofern der sich aus dem Profiling ergebende Informationswert die von der dritten Person vorgenommene Entscheidung maßgeblich beeinflusst und derart dem Betroffenen gegenüber rechtliche Wirkung entfaltet oder diesen in ähnlicher Weise erheblich beeinträchtigt.

5. Erkenntnis vom 3. September 2024, Ro 2022/04/0031

Im Ausgangsfall wurden auf einer Schulwebsite Daten der Lehrerschaft (Name, akademische Grade und Dienst-E-Mail) im Wissen der betroffenen Personen zugänglich gemacht. Die DSB wies eine diesbezügliche Beschwerde eines Lehrers aufgrund behaupteter Verletzung im Recht auf Geheimhaltung ab, da die Veröffentlichung dieser personenbezogenen Daten auf Art. 6 Abs. 1 lit. e DSGVO gestützt werden konnte. Dieser Ansicht hat sich – nach dem BVwG – auch der VwGH in seinem Erkenntnis angeschlossen. Maßgeblich für die Entscheidung ist § 56 Schulunterrichtsgesetz (SchUG), welcher die Schulleitung regelt, und insbesondere dessen Abs. 2, wonach der Schulleitung die Leitung der Schule sowie die Pflege der Verbindung zwischen der Schule, den Schüler:innen und den Erziehungsberechtigten sowie bei Berufsschulen auch den Lehrberechtigten obliegt. Die Aufgaben der Schulleitung umfassen demnach Schulleitung und –management, Qualitätsmanagement, Schul- und Unterrichtsentwicklung, Führung und Personalentwicklung sowie Außenbeziehungen und Öffnung der Schule.

Eine konkrete Datenverarbeitung ist darin nicht normiert, was sich laut VwGH aber als unerheblich erweist, da die von Art. 6 Abs. 1 lit. e DSGVO verlangten, im öffentlichen Interesse liegenden Aufgaben in § 56 SchUG ausreichend beschrieben werden und die gegenständliche Datenverarbeitung (dem Grunde nach) einer dieser Aufgaben gedient hat.

6. Erkenntnis vom 3. September 2024, Ra 2023/04/0106

In diesem Erkenntnis gab der VwGH der außerordentlichen Amtsrevision der DSB statt und hat das angefochtene Erkenntnis des BVwG aufgehoben. Auslöser für die Beschwerdeerhebung gegen eine Landesregierung war ein „Impferinnerungsschreiben", welches im Kopf das Landeswappen, den Schriftzug „Land […]" sowie die Bezeichnung „Amt der […] Landesregierung" aufwies.

Obwohl sich die Beschwerde gegen die Landesregierung richtete, führte die DSB das Verfahren, nach dem durch den Beschwerdeführer unbeantwortet gebliebenen Parteiengehör, gegen das Amt der Landesregierung als Beschwerdegegnerin, da sich dieses in einer Stellungnahme

ausdrücklich als datenschutzrechtlich Verantwortlicher deklarierte. Das BVwG führte in seiner den stattgebenden Bescheid der DSB ersatzlos behebenden Entscheidung aus, die DSB hätte, da nicht klar gewesen sei, wen dieser als Beschwerdegegnerin bezeichnen wolle, zunächst den Beschwerdeführer nach § 24 Abs. 2 Z 2 DSG iVm § 13 Abs. 3 zur Verbesserung anleiten müssen. Der VwGH erkannte, dass ein solcher Mängelbehebungsauftrag nur dann erforderlich gewesen wäre, wenn die DSB von einer Zumutbarkeit der Benennung des Beschwerdegegners ausgegangen wäre. Dies war gegenständlich aber nicht der Fall und das Erkenntnis des BVwG damit inhaltlich rechtswidrig.

5.4. Europäischer Gerichtshof für Menschenrechte

1. Urteil vom 11. Jänner 2024, Appl. Nr. 42541/18

Im Zuge eines internen Streits in der Führungsspitze einer spanischen politischen Partei waren E-Mails mit Daten des Beschwerdeführers in die Öffentlichkeit gelangt. Er erachtete sich durch die Beendigung der strafrechtlichen Ermittlungen in dieser Sache als in seinem Grundrecht gemäß Art. 8 EMRK verletzt.

Der EGMR wies die Beschwerde ab. Die Verfahrensbeendigung war in Spanien Gegenstand mehrerer, ausreichend begründeter Gerichtsentscheidungen.

2. Urteil vom 15. Mai 2024, Appl. Nr. 20949/21

Diese Beschwerde richtete sich gegen Nordmazedonien. Der als Kind adoptierten Beschwerdeführerin war seitens der Behörden unter Hinweis auf die nationale Rechtslage und das dort festgeschriebene Amtsgeheimnis jede Auskunft über ihre biologische Abstammung verweigert worden. Die Beschwerdeführerin konnte wegen einer bei ihr aufgetretenen, möglicherweise vererbbaren Erkrankung ein Interesse bescheinigen, mehr über ihre Abstammung zu erfahren.

Der EGMR stellte eine Verletzung im Grundrecht nach Art. 8 EMRK fest. Insbesondere, da die Behörden von Nordmazedonien nicht näher geprüft hatten, ob die biologischen Eltern einer Offenlegung ihrer Daten widersprochen hatten und weil das nationale Recht das entsprechende Amtsgeheimnis zu absolut und ohne die Möglichkeit von Ausnahmen festlegte.

3. Urteil vom 19. Dezember 2024, Appl. Nr. 29550/17

Gegenstand war die Durchsuchung der Räume einer Großloge der italienischen Freimaurer im Zuge einer parlamentarischen Anti-Mafia-Untersuchung. Dabei waren die personenbezogenen Daten von mehr als 6.000 Mitgliedern sichergestellt worden.

Der EGMR befand, dass die Maßnahme ohne ausreichende Begründung (Verdachtslage) angeordnet wurde sowie nicht zielgerichtet und überschießend war. Auch fehlte es in Italien an ausreichenden Garantien und Rechtsschutzmöglichkeiten („sufficient counterbalancing guarantees“) gegen Maßnahmen der gesetzgebenden Gewalt. Es wurde eine Verletzung der betroffenen Personen im Grundrecht nach Art. 8 EMRK festgestellt.

5.5. Gerichtshof der Europäischen Union

Auch der EuGH hat dieses Jahr zahlreiche Entscheidungen mit Relevanz für den Datenschutz getroffen. Die wichtigsten werden im Anschluss näher dargestellt. Ein Urteil betreffend einen parlamentarischen Untersuchungsausschuss bedingte sogar eine vom Österreichischen Nationalrat einstimmig beschlossene Anpassung des DSG, durch die in Österreich neben der Datenschutzbehörde ab Jänner 2025 erstmals eine weitere datenschutzrechtliche Aufsichtsbehörde ihren Betrieb aufnahm, das Parlamentarische Datenschutzkomitee (siehe dazu im Detail **Kapitel 3.2.**).

1. Urteil vom 16. Jänner 2024, C-33/22

Dem österreichischen Anlassverfahren lag die Veröffentlichung des Protokolls einer Befragung der beschwerdeführenden Partei vor einem vom Österreichischen Nationalrat eingesetzten Untersuchungsausschuss (betreffend das damalige Bundesamt für Verfassungsschutz und Terrorismusbekämpfung) zugrunde. Mit Bescheid vom 18. September 2019 erklärte sich die DSB für unzuständig und führte aus, dass der Grundsatz der Gewaltenteilung ausschließe, dass sie als Organ der Verwaltung die Tätigkeit eines derartigen Untersuchungsausschusses kontrolliert, welcher der Gesetzgebung zuzurechnen ist. Diese Entscheidung wurde vom BVwG infolge ersatzlos behoben. Der sodann vom VwGH im Wege der Vorabentscheidung angerufene EuGH hat entschieden, dass die Tätigkeit eines parlamentarischen Untersuchungsausschusses nicht von der Anwendung der DSGVO ausgenommen ist.

Der EuGH hat in seiner Entscheidung gewürdigt, dass mit Art. 2 Abs. 2 lit. a DSGVO, der vorsieht, dass die Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit findet, die nicht in den Anwendungsbereich des Unionsrechts fällt, allein Verarbeitungen vom Anwendungsbereich der Verordnung ausgenommen werden sollen, die von staatlichen Stellen im Rahmen der Wahrung der nationalen Sicherheit getätigt werden. Diese Auslegung ergibt sich weiters bereits daraus, dass in Art. 4 Z 7 DSGVO nicht danach unterschieden wird, wer Urheber der betreffenden Vereinbarung ist. Auch der Umstand, dass der Verantwortliche eine Behörde ist, deren Haupttätigkeit in der Gewährleistung der nationalen Sicherheit besteht, reicht als solcher nicht aus, um Verarbeitungen personenbezogener Daten, die diese Behörde im Rahmen ihrer anderen Tätigkeiten vornimmt, vom Anwendungsbereich der DSGVO auszunehmen. Die vom Untersuchungsausschuss ausgeübte politische Kontrolle stellt als solche keine Tätigkeit dar, die unter Art. 2 Abs. 2 lit. a DSGVO fällt.

Aufgrund des Vorrangs des Unionsrechts kann sich ein Mitgliedstaat, der sich für die Einrichtung einer einzigen Datenschutzaufsichtsbehörde entschieden hat, nicht auf Bestimmungen des nationalen (Verfassungs)Rechts berufen, um die Verarbeitung personenbezogener Daten, die in den Anwendungsbereich der DSGVO fällt, der Überwachung durch diese Behörde zu entziehen.

2. Urteil vom 25. Jänner 2024, C-687/21

Im gegenständlichen Anlassverfahren hat eine betroffene Person bei einem Elektromarktunternehmen ein Elektrohaushaltsgerät mittels Kauf- und Kreditvertrag erworben, die dazugehörige Rechnung ist allerdings von einem Mitarbeiter der Verantwortlichen irrtümlich einem anderen Kunden ausgehändigt worden. Die betroffene Person verlangte vor einem deutschen Gericht sodann immateriellen Schadenersatz gemäß Art. 82 DSGVO. Das deutsche Gericht stellte sieben Vorfragen an den EuGH. Zwei der Vorfragen hat der EuGH dahingehend beantwortet, dass

Art. 5 (Grundsätze für die Verarbeitung personenbezogener Daten), Art. 24 (Verantwortung des für die Verarbeitung Verantwortlichen), Art. 32 (Sicherheit der Verarbeitung) und Art. 82 DSGVO zusammen betrachtet dahingehend auszulegen sind, dass im Rahmen einer auf Art. 82 DSGVO gestützten Schadenersatzklage der Umstand, dass Mitarbeiter der Verantwortlichen irrtümlich ein Dokument mit personenbezogenen Daten an einen unbefugten Dritten weitergegeben hat, für sich genommen nicht ausreicht, um davon auszugehen, dass die technischen und organisatorischen Maßnahmen für die Datenverarbeitung nicht „geeignet" iSv Art. 24 und 32 DSGVO waren.

Eine Frage beantwortete der EuGH damit, dass Art. 82 DSGVO, insbesondere im Falle eines immateriellen Schadens, eine Ausgleichsfunktion haben soll, um den erlittenen Schaden vollständig auszugleichen, und keine Straffunktion erfüllt. Weiters erklärte er, dass Art. 82 DSGVO nicht verlangt, dass die Schwere des Verstoßes der Verantwortlichen für die Höhe des Schadenersatzes berücksichtigt wird. Außerdem muss die betroffene Person, um Art. 82 Abs. 1 DSGVO geltend zu machen, nicht nur den Verstoß gegen die DSGVO nachweisen, sondern auch, dass ihr dadurch ein (immaterieller) Schaden entstanden ist.

Zuletzt stellte der EuGH noch klar, dass Art. 82 Abs. 1 DSGVO dahingehend auszulegen ist, dass nicht schon deshalb ein „immaterieller" Schaden vorliegt, weil die Person hypothetisch befürchtet, dass im Anschluss an die Weitergabe der personenbezogenen Daten an einen unbefugten Dritten in der Zukunft eine Weiterverbreitung oder ein Missbrauch der Daten stattfinden könnte.

3. Urteil vom 7. März 2024, C-604/22

In diesem vor den EuGH gebrachten Fall ging es um einen Verband, welcher einen Regelungsrahmen schaffte, der die Verarbeitung personenbezogener Daten von betroffenen Personen auf Websites oder Anwendungen im Einklang mit der DSGVO sicherstellen sollte. Dieser Rahmen erleichtere die Erfassung der Nutzerpräferenzen und Einwilligungen/Widersprüchen durch u.a. ihre Kodierung und Speicherung in einem String („TC-String"), bestehend aus einer Kombination von Buchstaben und Zeichen. Gleichzeitig wird, damit der String zuordenbar ist, ein Cookie auf dem Nutzer:innen-Gerät gespeichert. Der String wird sodann auf einer Plattform mit den am Verband beteiligten Brokern personenbezogener Daten und Werbeplattformen geteilt.

Der EuGH sprach aus, dass auch diese Kombination aus Buchstaben und Zeichen als Information über die betroffene Person und bei möglicher Identifizierbarkeit über die IP-Adresse deren personenbezogenes Datum ist. Dem steht auch nicht entgegen, dass der Verband nicht selbst den String mit der IP-Adresse des Nutzer:innen-Geräts kombinieren kann und nicht über die Möglichkeit verfügt, unmittelbar auf die im Rahmen des Regelungswerks verarbeiteten personenbezogenen Daten zuzugreifen.

Weiters befasste sich der Gerichtshof mit einer allfälligen gemeinsamen Verantwortlichkeit des Verbandes und seiner Mitglieder. Hierzu beurteilte er, ob diese Organisation aus Eigeninteresse auf die Verarbeitung personenbezogener Daten, wie des Strings, Einfluss nimmt und damit gemeinsam mit seinen Mitgliedern die Zwecke und Mittel solcher Vorgänge festlegt. Der EuGH bejahte das grundsätzlich, da der vom Verband geschaffene Regelungsrahmen den Verkauf und Kauf von Werbeflächen durch Online-Versteigerung fördern und ermöglichen soll und damit den Zweck der Verarbeitung (gemeinsam mit den Mitgliedern) festlegt. Da dieses Regelungswerk weiters von Mitgliedern des Verbandes zwingend einzuhalten ist und technische Spezifikationen für die Verarbeitung des Strings sowie dessen Inhalte regelt, werden auch die Mittel

gemeinsam von dem Verband und seinen Mitgliedern bestimmt und ist der Verband damit gemeinsamer Verantwortlicher für die Verarbeitungen des Strings.

4. Urteil vom 7. März 2024, C-740/22

Im Anlassverfahren hat ein international operierendes Fernsehproduktionsunternehmen beim finnischen Gericht erster Instanz mündlich Auskunft über möglicherweise verhängte oder bereits verbüßte Strafen einer betroffenen Person gefordert, welche an einem vom Unternehmen organisierten Wettbewerb teilnahm. Das finnische Gericht wies den Antrag zurück, da kein im finnischen Datenschutzgesetz normierter Grund für eine Verarbeitung strafrechtlicher Daten vorlag und auch ein Suchlauf in den Informationssystemen dieses Gerichts eine Verarbeitung personenbezogener Daten dargestellt hätte, weshalb die beantragten Informationen auch mündlich nicht mitgeteilt werden konnten. Letztendlich stellte das Berufungsgericht an den EuGH insbesondere die Frage, ob auch eine mündliche Übermittlung personenbezogener Daten eine Verarbeitung personenbezogener Daten iSv Art. 2 Abs. 1 und Art. 4 Z 2 DSGVO darstellt.

Der EuGH führte dazu aus, dass aus dem Ausdruck „jeder Vorgang“ im „Verarbeitung“ definierenden Art. 4 Z 2 DSGVO der Unionsgesetzgeber den Begriff „Verarbeitung“ weit fassen wollte, was dadurch bestätigt wird, dass die Aufzählung der dort genannten Vorgänge nicht abschließend ist, was durch die Wendung „wie“ zum Ausdruck kommt. Die Aufzählung erfasst u.a. die Offenlegung durch Übermittlung, die Verbreitung und „[jede] andere Form der Bereitstellung“. Diese Vorgänge können automatisiert oder nicht automatisiert erfolgen und stellt Art. 4 Z 2 DSGVO auch keine Bedingungen für die „nicht automatisierte“ Verarbeitung, wodurch eine mündliche Übermittlung jedenfalls abgedeckt sei. Auch der in Art. 2 DSGVO definierte Anwendungsbereich der DSGVO, welcher lediglich „ganz oder teilweise automatisierte Verarbeitungen personenbezogener Daten“ sowie „nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“ umfasst, ist geprüft worden. Da die mündliche Übermittlung eine nicht automatisierte Verarbeitung darstellt, ist es erforderlich, dass die Daten, die Gegenstand dieser Verarbeitung sind, in einem „Dateisystem“ gespeichert sind oder gespeichert werden sollen, um in den sachlichen Anwendungsbereich der DSGVO zu fallen. Der EuGH hat die Vorlage sohin dahingehend beantwortet, dass eine mündliche Auskunft über möglicherweise verhängte oder bereits verbüßte Strafen in Bezug auf eine natürliche Person eine Verarbeitung personenbezogener Daten darstellt, die in den sachlichen Anwendungsbereich der DSGVO fällt, wenn diese Informationen in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Der EuGH sprach im Urteil weiters aus, dass die in Art. 85 DSGVO verankerte Informationsfreiheit nicht dahingehend ausgelegt werden kann, dass diese die Preisgabe von personenbezogenen Daten über strafrechtliche Verurteilungen an jede Person rechtfertigt, die sie beantragt. Die Informationen begehrende Person, unabhängig davon ob es sich dabei um ein Unternehmen oder eine Privatperson handelt, muss vielmehr ein besonderes Interesse an diesen Daten geltend machen. Umgekehrt stellt der Zugang der Öffentlichkeit zu amtlichen Dokumenten ein öffentliches Interesse dar, welches eine solche Verarbeitung rechtfertigen kann und steht die DSGVO der Informationsfreiheit nicht entgegen. Bei der Rechtmäßigkeitsüberprüfung iSv Art. 6 Abs. 1 lit. e DSGVO der Übermittlung der personenbezogenen Daten an die Öffentlichkeit ist allerdings zu prüfen, ob sie angesichts der Schwere des Grundrechtseingriffes in die Privatsphäre und den Schutz personenbezogener Daten im Hinblick auf die Verwirklichung der verfolgten Ziele gerechtfertigt und insbesondere verhältnismäßig ist.

5. Urteil vom 26. September 2024, C-768/21

In dieser Sache verlangte eine betroffene Person von der zuständigen deutschen Datenschutzaufsichtsbehörde deren Tätigwerden, nachdem sie von einer Datenschutzverletzung („Data Breach", Art. 33 DSGVO) bei ihrer Hausbank Kenntnis erlangt hatte. Die Aufsichtsbehörde, die eine entsprechende Meldung der Bank erhalten, den Vorfall geprüft und keinen Grund für zusätzliche behördliche Abhilfemaßnahmen gefunden hatte, lehnte dies ab. Die betroffene Person klagte dagegen beim zuständigen Verwaltungsgericht und beantragte, die Aufsichtsbehörde zum Einschreiten, insbesondere zur Verhängung einer Geldbuße gegen die Bank, zu verpflichten.

Auf Vorabentscheidungsersuchen des Verwaltungsgerichts urteilte der EuGH, dass Art. 57 Abs. 1 lit. a und f, Art. 58 Abs. 2 sowie Art. 77 Abs. 1 DSGVO dahin auszulegen sind, dass die Aufsichtsbehörde im Fall der Feststellung einer Verletzung des Schutzes personenbezogener Daten nicht verpflichtet ist, nach Art. 58 Abs. 2 eine Abhilfemaßnahme zu ergreifen, insbesondere eine Geldbuße zu verhängen, wenn ein solches Einschreiten nicht geeignet, erforderlich oder verhältnismäßig ist, um der festgestellten Unzulänglichkeit abzuhelfen und die umfassende Einhaltung dieser Verordnung zu gewährleisten. Dabei sind auch vom Verantwortlichen bereits selbst ergriffene Maßnahmen zu berücksichtigen.

6. Urteil vom 4. Oktober 2024, C-507/23

In diesem Urteil in einem aus Lettland vorgelegten Vorabentscheidungsverfahren war die Schadenersatzbestimmung des Art. 82 DSGVO Gegenstand der Auslegung. Ein lettischer Journalist lag im Streit mit der Verbraucherschutzbehörde (PTAC), weil er sich in einer von dieser produzierten und verbreiteten Videosequenz für verspottet erachtete. Er verlangt u.a. gestützt auf Art. 82 DSGVO, Schadenersatz.

Der EuGH legte die Bestimmung dahingehend aus, dass ein einfacher Verstoß gegen die DSGVO noch keinen Schaden darstellt, auch eine Entschuldigung ein angemessener Ersatz eines immateriellen Schadens sein kann und dass Haltung und Beweggründe des Verantwortlichen keine Gründe für eine Minderung eines Ersatzanspruchs bilden.

7. Urteil vom 4. Oktober 2024, C-21/23

In dieser Sache (Hintergrund: wettbewerbsrechtlicher Streit zwischen einer ortsgebunden tätigen Apotheke und einer Apotheke, die rezeptfreie Medikamente über eine internationale Online-Plattform vertreibt) hat der EuGH im Zuge eines Vorabentscheidungsersuchens aus Deutschland klargestellt, dass eine wettbewerbsrechtliche Klage auch darauf gestützt werden kann, dass ein Mitbewerber bei der Verarbeitung von Kundendaten gegen die DSGVO verstößt. Personenbezogene Daten betreffend eine Online-Bestellung rezeptfreier Arzneimittel sind besonders geschützte Gesundheitsdaten gemäß Art. 9 Abs. 1 DSGVO.

8. Urteil vom 4. Oktober 2024, C-621/22

Ein Sport-Dachverband hatte mit einem Sponsor (Anbieter von Wetten und Glücksspielen) vereinbart, ihm Daten seiner Mitglieder für Zwecke der Direktwerbung zur Verfügung zu stellen. Im daraus resultierenden Datenschutz-Streitfall zog der EuGH auf Vorabentscheidungsersuchen eines Gerichts aus den Niederlanden die Grenzen einer auf Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen) gestützten Datenverarbeitung eng: Eine Verfolgung wirtschaftlicher Interessen des Verantwortlichen kann in diesem Fall zwar berechtigt sein, dies jedoch nur

dann, wenn die Verarbeitung zur Verwirklichung des in Rede stehenden berechtigten Interesses absolut notwendig ist und sofern in Anbetracht aller relevanten Umstände die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen gegenüber dem berechtigten Interesse nicht überwiegen. Art. 6 Abs. 1 lit. f DSGVO verlangt zwar nicht, dass ein solches Interesse gesetzlich bestimmt wird, die Bestimmung erfordert jedoch, dass das geltend gemachte berechtigte Interesse rechtmäßig ist, also gegen kein Gesetz verstößt. Die vom Datenempfänger verfolgten Geschäftszwecke (Aspekt der Gefährdung durch Spielsucht) sind in die Interessenabwägung einzubeziehen.

Eine ähnliche Fragestellung war bereits im Urteil vom 12. September 2024, C-17/22, zu beantworten.

9. Urteil vom 4. Oktober 2024, C-446/21

Ein bekannter Aktivist hatte in einer öffentlichen Podiumsdiskussion Angaben zu seiner sexuellen Orientierung gemacht. Der Betreiber und Verantwortliche eines großen Sozialen Netzwerks verarbeitete Daten dazu ohne Einwilligung des Betroffenen für den Zweck der zielgerichteten Online-Werbung. Gegen diese Verarbeitung seiner Daten ging der Betroffene (als registrierter User des betreffenden Netzwerks) in Österreich vor den Zivilgerichten nach Art. 79 DSGVO vor. Der OGH legte schließlich dem EuGH mehrere Fragen zur Vorabentscheidung vor.

In Auslegung von Art. 5 Abs. 1 und Art. 9 DSGVO urteilte der EuGH, dass der Grundsatz der „Datenminimierung“ (Art. 5 Abs. 1 lit. c DSGVO) es nicht gestattet, dass sämtliche personenbezogenen Daten, die ein Verantwortlicher für ein soziales Netzwerk von der betroffenen Person oder von Dritten erhält und die sowohl auf als auch außerhalb dieser Plattform erhoben wurden, zeitlich unbegrenzt und ohne Unterscheidung nach ihrer Art für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet werden. Art. 9 Abs. 2 lit. e DSGVO ist nicht so zu verstehen, dass jemand, der eine Tatsache einmalig öffentlich erwähnt hat, diese Tatsache „offensichtlich öffentlich gemacht“ und damit die Verarbeitung von Daten dazu für Werbezwecke erlaubt hat.

10. Urteil vom 4. Oktober 2024, C-548/21

Im Zuge einer Maßnahmenbeschwerdesache (Ermittlungen wegen Verdachts einer Straftat nach § 27 Abs. 1 Suchtmittelgesetz polizeiliche Sicherstellung eines Mobiltelefons, Versuche der Kriminalpolizei, das Gerät zu entsperren und Zugang zu den gespeicherten Daten zu erlangen) legte das LVwG Tirol dem EuGH Fragen betreffend die Auslegung der DSRL-PJ vor.

Da es bei einem Versuch blieb und auf die im Handy vorhandenen Daten nicht zugegriffen wurde, beschäftigte sich der EuGH zunächst mit der Anwendbarkeit der DSRL-PJ. Er bejahte ihre Anwendbarkeit unter Hinweis darauf, dass der Unionsgesetzgeber den sachlichen Anwendungsbereich der Richtlinie möglichst weit fassen wollte und dass jede anders ausfallende Auslegung dem beabsichtigten hohen Schutzniveau für personenbezogene Daten zuwiderlaufen würde. Eine solche Auslegung würde die von einem Zugriffsversuch betroffenen Personen nämlich einer erheblichen Gefahr aussetzen, dass ein Verstoß gegen die in dieser Richtlinie aufgestellten Grundsätze nicht mehr verhindert werden kann. Auch bei einer beabsichtigten Datenverarbeitung wie im gegenständlichen Fall ist die Anwendbarkeit der Richtlinie also zu bejahen.

Der EuGH legte die Art. 4 Abs. 1 lit. c, 13 und 54 DSRL-PJ sodann im Lichte der Art. 7 und 8 sowie von Art. 52 Abs. 1 der EU-GRC so aus, dass diese einer nationalen Regelung, die den

zuständigen Behörden die Möglichkeit gibt, zum Zweck der Strafverfolgung auf die auf einem Mobiltelefon gespeicherten Daten zuzugreifen, nicht entgegenstehen, wenn diese Regelung die Art oder die Kategorien der betreffenden Straftaten hinreichend präzise definiert, die Wahrung des Grundsatzes der Verhältnismäßigkeit gewährleistet und die Ausübung dieser Möglichkeit, außer in hinreichend begründeten Eilfällen, einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterwirft. Die betroffene Person muss jedoch informiert werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet werden könnte.

11. Urteil vom 28. November 2024, C-169/23

In dieser Sache, die ihren Ausgang in Ungarn genommen hatte (Streit um die elektronische Verarbeitung von Impfdaten für Covid19-Immunitätszertifikate) hat der EuGH entschieden, dass auch vom Verantwortlichen selbst generierte Daten unter die Ausnahme von der Informationspflicht gemäß Art. 14 Abs. 5 lit. c DSGVO fallen. Im Rahmen der Behandlung einer entsprechenden Beschwerde darf die Aufsichtsbehörde nicht die Geeignetheit von Maßnahmen zum Schutz der Datensicherheit (Art. 32 DSGVO) prüfen.

6. Europäische Zusammenarbeit

6.1. Europäische Union

6.1.1 Der Europäische Datenschutzausschuss

Im EDSA wurde im Jahr 2024 eine der beiden Positionen des stellvertretenden Vorsitzenden neu besetzt, da die Amtszeit eines der beiden stellvertretenden Vorsitzenden planmäßig am 15. Mai 2024 endete. Im Rahmen des Wahlgangs wurde der **Leiter der kroatischen Datenschutzaufsichtsbehörde, Zdravko Vukić**, für die nächsten fünf Jahre in das zweite Amt des **stellvertretenden Vorsitzenden** gewählt und folgt in dieser Funktion dem Leiter der niederländischen Datenschutzaufsichtsbehörde, Aleid Wolfsen, nach. Der übrige Vorsitz im EDSA hat 2024 keine Änderung erfahren.

Die **Vollversammlung des EDSA** hat sich im Jahr 2024 insgesamt **zwölf Mal getroffen**, wobei eine Versammlung außerordentlich einberufen wurde. Es fanden fünf Treffen vor Ort in Brüssel statt und sieben Treffen wurden via Videokonferenz abgehalten.

Die im Rahmen dieser Treffen besprochenen Themen und angenommenen Dokumente wurden in den Experten-Untergruppen des EDSA vorbereitet, die einander im Jahr 2024 im Rahmen ihrer regelmäßigen Arbeitssitzungen sowohl vor Ort in Brüssel als auch per Videokonferenz getroffen haben. Eine Auswahl dieser Dokumente wird im Folgenden näher dargelegt.

Der EDSA hat gemäß **Art. 64 DSGVO** im Jahr 2024 insgesamt **28 Stellungnahmen**[34] zu folgenden Themen abgegeben:

- 15 Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (Booking.com, Telefónica Group, Accenture Group, MAPFRE Group, Genpact Group, Ivoclar Vivadent Group, Mercans Group, 2 Mal AVATURE Group, FCC Group, Viega Group, Talan Group, Aptiv Group, Infosys Group)
- 1 Stellungnahme zum Begriff der Hauptniederlassung eines Verantwortlichen in der Union (EDPB Opinion 04/2024)
- 1 Stellungnahme zur Wirksamkeit von Einwilligungen im Kontext von Consent-or-Pay Modellen großer Online-Plattformen (EDPB Opinion 08/2024)
- 1 Stellungnahme zu bestimmten Pflichten beim Einsatz von Auftragsverarbeitern und Subauftragsverarbeitern (EDPB Opinion 22/2024)
- 1 Stellungnahme zum Einsatz von Gesichtserkennung zur Straffung der Fluggastströme (EDPB Opinion 11/2024)
- 1 Stellungnahme zu bestimmten Aspekten der Verarbeitung personenbezogener Daten im Rahmen von KI-Modellen (EDPB Opinion 28/2024)
- 3 Stellungnahmen zu nationalen Zertifizierungskriterien (2 Mal Deutschland, Österreich)
- 1 Stellungnahme zu einem Europäischen Datenschutzsiegel
- 1 Stellungnahme zum Entwurf der Akkreditierungsanforderungen für eine Zertifizie-

34 Siehe hierzu https://www.edpb.europa.eu/our-work-tools/consistency-findings/opinions_de?f%5B0%5D=opinions_date%3A2024.

rungsstelle gemäß Art. 43 DSGVO (Schweden)
- 1 Stellungnahme zu nationalen Verhaltensregeln (Frankreich)
- 1 Stellungnahme zu nationalen Ausnahmen von der Datenschutz-Folgenabschätzung (Lettland)
- 1 Stellungnahme zur Zertifizierung der IT-gestützten Verarbeitung personenbezogener Daten gem. Art. 42 DSGVO (Deutschland)

Zudem hat der EDSA im Jahr 2024 zu folgenden Themen **Leitlinien**[35] verabschiedet:

- Zur Verarbeitung personenbezogener Daten auf Grundlage von berechtigten Interessen (EDPB Guidelines 01/2024)
- Zu Art. 48 DSGVO (EDPB Guidelines 02/2024)

Des Weiteren wurden zu folgenden Themen **endgültige Fassungen von Leitlinien** angenommen:

- Zu Art. 37 der RL (EU) 2016/680 (EDPB Guidelines 01/2023, Version 2.1)
- Zum technischen Anwendungsbereich von Art. 5 Abs. 3 der RL 2002/58/EG (EDPB Guidelines 02/2023, Version 2.0)

Auch im Jahr 2024 wurden *alle* Expertenuntergruppen des EDSA seitens der DSB beschickt, jede Expertenuntergruppe traf sich in der Regel mindestens einmal im Monat in Brüssel oder per Videokonferenz zur Besprechung und Vorbereitung der Arbeit des EDSA.

Im Jahr 2024 hatte sich der EDSA gleich mehrmals mit **Anträgen von Datenschutzaufsichtsbehörden nach Art. 64 Abs. 2 DSGVO** zu befassen. Nach dieser Bestimmung kann dem EDSA von einer Aufsichtsbehörde, dem Vorsitz des Datenschutzausschusses oder der Europäischen Kommission eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vorgelegt und die Erlassung einer Stellungnahme beantragt werden. Zwei Stellungnahmeverfahren standen im Jahr 2024 besonders im Fokus der Öffentlichkeit und werden im Nachfolgenden näher erläutert:

Zunächst widmete sich der EDSA einem Antrag der Datenschutzaufsichtsbehörden der Niederlande, Norwegen und Hamburg betreffend sog. **Einwilligungs- oder Bezahlmodelle von großen Online-Plattformen („pay or ok")**. Darunter ist die mittlerweile weit verbreitete Praxis zahlreicher Online-Plattformen zu verstehen, für ihre Dienstleistungen entweder eine Einwilligung zur Verarbeitung personenbezogener Daten der Nutzer:innen für bestimmte Zwecke (meist Werbezwecke) oder die Zahlung einer bestimmten Gebühr zu verlangen.

Obwohl der EDSA zur Ansicht gelangte, dass der Einsatz von Einwilligungs- oder Bezahlmodellen durch große Online-Plattformen unter Berücksichtigung der Rechtsprechung des EuGH dem Grunde nach nicht verboten ist, hielt er fest, dass es großen Online-Plattformen in den meisten Fällen nicht möglich sein wird, die Anforderungen an eine gültige Einwilligung zu erfüllen, wenn sie ihren Nutzer:innen lediglich die Wahl zwischen der Erteilung einer Einwilligung in die Verarbeitung ihrer personenbezogenen Daten für verhaltensbezogene Werbezwecke oder

35 Siehe hierzu https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de?f%5B0%5D=opinions_date%3A2024.

der Zahlung einer Gebühr lassen. Der EDSA empfahl daher, von rein dualen Auswahlmöglichkeiten, die lediglich eine Wahl zwischen einer kostenpflichtigen Variante ohne verhaltensbasierte Werbung oder einer Variante mit Einwilligung für verhaltensbezogene Werbezwecke bieten, abzusehen und bspw. zusätzlich eine weitere kostenlose Alternative ohne verhaltensbezogene Werbung anzubieten.

Im Ergebnis stellt diese Stellungnahme – obwohl auf große Online-Plattformen beschränkt – eine wichtige Richtschnur für die Beurteilung der Zulässigkeit von Einwilligungs- oder Bezahlmodellen im Online-Bereich dar. Aufgrund der Wichtigkeit dieser Thematik hat der EDSA ergänzend auch ein Mandat für die Erarbeitung von Leitlinien zu diesem Thema beschlossen.

In einem weiteren Fall wurden von der irischen Datenschutzaufsichtsbehörde an den EDSA Fragen betreffend die **Verarbeitung personenbezogener Daten im Rahmen von KI-Modellen** herangetragen. In seinem Kern befasste sich der Antrag mit den Fragen, ob und inwieweit dabei ein Personenbezug besteht, ob eine unrechtmäßige Verarbeitung während der Lernphase eines KI-Modells auf nachfolgende Anwendungsphasen durchschlägt und unter welchen Voraussetzungen berechtigte Interessen als Verarbeitungsgrundlage herangezogen werden können. Im Rahmen dieses Stellungnahmeverfahrens wurde auch zum ersten Mal eine öffentliche Konsultation abgehalten, in welcher interessierte Stakeholder vorab ihre Positionen mit dem EDSA teilen und diskutieren konnten.

Der EDSA gab in seiner Stellungnahme etliche Beispiele betreffend die Interessenabwägung bei derartigen Datenanwendungen und kam zum Ergebnis, dass die an ihn gerichteten Fragen einer Einzelfallbeurteilung der zuständigen Aufsichtsbehörde bedürfen, da sie aufgrund der schieren Anzahl an Anwendungsmöglichkeiten von KI nicht pauschal beantwortet werden können. Zu weiteren Aspekten der Verarbeitung personenbezogener Daten im Rahmen von KI-Anwendungen werden vom EDSA Leitlinien ausgearbeitet.

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. Zu diesem Zweck ist Europol ermächtigt, eine große Menge von vor allem strafrechtsrelevanten Daten zu verarbeiten. Die Aufgaben und Befugnisse sowie die Kontrolle der Verarbeitung von personenbezogenen Daten durch Europol sind durch die **Verordnung 2016/794**[36], zuletzt geändert durch die **Verordnung 2022/991**[37], geregelt. Die Kontrollbefugnis obliegt einerseits den nationalen Kontrollbehörden, in Österreich ist dies die DSB, sowie andererseits dem EDSB.

Während die nationalen Kontrollbehörden die Zulässigkeit der Eingabe und des Abrufs personenbezogener Daten sowie jedweder Übermittlung dieser Daten an Europol überwachen, obliegt dem EDSB die Überwachung der Verarbeitung durch Europol selbst. Jede betroffene Person kann beim EDSB 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.

36 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0794.
37 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R0991.

Um eine möglichst effiziente und einheitliche Kontrolle innerhalb der Mitgliedstaaten zu gewährleisten, treffen sich Vertreter:innen der nationalen Kontrollbehörden sowie des EDSB in regelmäßigen Abständen im Rahmen eines Komitees (**„Coordinated Supervision Committee“**). Aufgabe dieses Komitees ist es, u.a. allgemeine Richtlinien und Strategien zur Überwachung von Europol zu erarbeiten und die Vorgehensweise der nationalen Aufsichtsbehörden bei der Prüfung der Zulässigkeit der Verarbeitung und der Übermittlung von personenbezogenen Daten durch die nationalen Europolstellen an Europol zu akkordieren.

Der **EDSB konsultierte die DSB** im Jahr 2024 **in einem Fall** zum Zweck der Zusammenarbeit im Zuge von beim EDSB gegen Europol eingebrachten Beschwerden, wobei die DSB im Rahmen dieses Konsultationsverfahrens die Rechtmäßigkeit der Verarbeitung sowie die Übermittlung der Daten der Betroffenen durch österreichische Sicherheitsbehörden an Europol zu überprüfen hatte.

6.1.3 Schengen (einschließlich Teilnahme an Schengen-Evaluierungen) sowie Visa

Das **Schengener Informationssystem (SIS)** ermöglicht EU-weit und in assoziierten Schengen – Ländern (bspw. Schweiz, Norwegen) die Ausschreibungen von Personen (bspw. vermisste Personen) und Gegenständen (etwa gestohlene Reisedokumente) in einer gemeinsamen Datenbank, die von nationalen Behörden wie Polizei und Grenzschutz eingegeben und in Echtzeit abgefragt werden können.

2013 wurde das **Schengener Informationssystem der zweiten Generation (SIS II)** eingeführt, im März 2023 **wurde das SIS erneuert** und wurden bspw. neue Ausschreibungsarten hinzugefügt (etwa Ausschreibungen zur Einreise- und Aufenthaltsverweigerung in einem Mitgliedsstaat).

Die Rechtsgrundlagen für das SIS sind in drei unmittelbar anwendbaren Verordnungen der Europäischen Union geregelt[38].

Die durch die EU-Verordnungen des Schengener Informationssystems eingerichteten spezialisierten **nationalen SIRENE-Büros** (in Österreich beim Bundeskriminalamt situiert) sind zentrale Anlaufstellen für den Austausch zusätzlicher Informationen und der Koordinierung von Aktivitäten mit Behörden anderer Mitgliedsstaaten im Zusammenhang mit SIS-Ausschreibungen.

Um die Rechte Betroffener sicherzustellen, hat die Europäische Union in den Verordnungen Auskunfts-, Berichtigungs- und Löschungsrechte (bei unrechtmäßiger Verarbeitung) festgelegt. Diese können im Streitfall vor den nationalen Datenschutzbehörden oder vor den ordentlichen Gerichten geltend gemacht werden.

Das SIS[39] besteht aus einem EU-weiten zentralen System (sog. **C.SIS**), den jeweiligen nationalen Systemen der Mitgliedstaaten (sog. **N.SIS**) sowie einer Kommunikationsinfrastruktur zwischen dem zentralen System und den nationalen Systemen.

38 Verordnung (EU) 2018/1860 über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger; Verordnung (EU) 2018/1861 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen; Verordnung (EU) 2018/1862 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen.

39 https://home-affairs.ec.europa.eu/system/files/2023-04/SIS%20leaflet-online%20version_DE.pdf.

Eine weitere wesentliche Anwendung ist das sogenannte **Visa-Informationssystem (VIS)**, das die Umsetzung der gemeinsamen EU-Visumpolitik unterstützt, indem es den Austausch von Visa-Daten zwischen den Mitgliedstaaten der Europäischen Union sowie assoziierten Ländern ermöglicht.

Das VIS verarbeitet Daten im Zusammenhang mit Anträgen auf Erteilung eines Visums für den kurzfristigen Aufenthalt zum Besuch oder zur Durchreise durch den Schengen-Raum. 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**[40].

Das VIS besteht – ähnlich wie das SIS - aus einem **EU-weiten zentralen System** (**C.VIS**), den allfälligen nationalen Systemen der Mitgliedstaaten sowie einer Kommunikationsinfrastruktur zwischen dem zentralen System und den nationalen Systemen.

Die jeweiligen nationalen Datenschutzbehörden haben gemäß der SIS-Verordnungen bzw. der VIS-Verordnung die Rechtmäßigkeit der Verarbeitung personenbezogener SIS-Daten bzw. VIS–Daten auf nationaler Ebene zu überwachen, wobei in wiederkehrenden Intervallen die Datenverarbeitungsvorgänge auf nationaler Ebene nach internationalen Prüfungsstandards zu überprüfen sind.

Im Rahmen des **VIS–Audits** wurde die Anwendung des VIS durch Bedienstete der DSB mittels standardisierten Fragebogens und Prozedere in den österreichischen **Konsulaten bzw. Botschaften in Bratislava, Tirana, Sarajevo, Laibach und Belgrad** vorgenommen, wie mit Durchführungsbeschluss des Rates der Europäischen Union vom 17. Juni 2022 zu **Zl. 10396/22**[41] zur Beseitigung der im Jahr 2020 bei der Evaluierung festgestellten Mängel empfohlen.

Darüber hinaus überprüft die Europäische Kommission gemeinsam mit nationalen Experten die Umsetzung der SIS-Verordnungen bzw. der VIS-Verordnung in den einzelnen Mitgliedstaaten.

Eine derartige Überprüfung in den Bereichen „Datenschutz“ und „Polizei“ wird für die Republik Österreich neuerlich im Mai 2025 stattfinden. Die Vorbereitungen dafür sind im vollen Gange.

Darüber hinaus haben im Berichtszeitraum für das Jahr 2024 Bedienstete der DSB an den Schengen Evaluierungen der Länder Kroatien und Tschechien teilgenommen. Auch für das Jahr 2025 ist die Teilnahme an Schengen-Evaluierungen in den Mitgliedsstaaten durch die DSB vorgesehen.

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. Grundlage ist die Verordnung **(EG) 515/97**.[42]

Zur Gewährleistung eines angemessenen Datenschutzes wurde neben dem Ausschuss (**„Joint Supervisory Authority of Customs“ („JSA“)**) eine Koordinierende Aufsichtsbehörde (**CIS Supervision Coordination Group („CIS-SCG“)**) eingerichtet, welche aus Vertreter:innen der nationalen

40 https://eur-lex.europa.eu/DE/legal-content/summary/vis-regulation.html.
41 https://data.consilium.europa.eu/doc/document/ST-10396-2022-INIT/en/pdf.
42 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:01997R0515-20210101.

Datenschutzaufsichtsbehörden der Mitgliedstaaten und dem EDSB gebildet wird. Damit in Zukunft zur koordinierten Überwachung der EU-Systeme im Bereich Datenschutz ein einheitliches Forum besteht, ist beabsichtigt, dass die Aufgaben der koordinierenden Aufsichtsbehörde (**CIS Supervision Coordination Group („CIS-SCG")** von beim EDSA eingerichteten Komitee (**Coordinated Supervision Committee (CSC)**) übernommen werden.

6.1.5 Eurodac

Das Eurodac System ermöglicht den Einwanderungsbehörden der Mitgliedstaaten Asylwerber:innen und andere Personen zu identifizieren, die beim illegalen Überschreiten einer EU-Außengrenze aufgegriffen werden. Anhand der Fingerabdrücke kann ein Mitgliedstaat feststellen, ob eine:ein Fremde:r in einem anderen Mitgliedstaat Asyl beantragt hat oder, ob ein:eine Asylwerber:in illegal in die EU eingereist ist. Grundlage für den Einsatz von Eurodac ist die **Verordnung 603/2013**.[43]

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. 603/201347** sieht eine koordinierte Überwachung durch die nationalen Datenschutzbehörden mit dem EDSB vor, wobei die Mitgliedstaaten jährlich eine Überprüfung der Verarbeitung personenbezogener Daten durchzuführen haben. Zu diesem Zweck wurde die Eurodac Supervision Coordination Group gegründet, mit dem Ziel, eine koordinierte Überwachung der EU-Systeme im Bereich Datenschutz sicherzustellen. Zukünftig soll diese Aufgabe vom durch den EDSA eingerichteten Komitee CSC übernommen werden.

Die DSB als nationale Kontrollbehörde leitete im Jahr 2023 **ein amtswegiges Prüfverfahren** betreffend den Einsatz von Eurodac durch nationale Behörden ein. Dieses Verfahren ist noch anhängig, ein zeitnaher Abschluss ist zu erwarten.

6.2. Europarat

Die DSB vertrat die Republik Österreich im Ausschuss nach **Art. 18 (T-PD) der Datenschutzkonvention des Europarates (EVS Nr. 108, BGBl. Nr. 317/1988)**.

Im Berichtszeitraum fanden von 5. bis 7. Juni 2024 die 46. Plenarsitzung und von 4. bis 6. November 2024 die 47. Plenarsitzung des T-PD in Straßburg statt. Die Tagesordnung sowie der zusammenfassende Bericht der Sitzungen sind in englischer Sprache unter https://www.coe.int/en/web/data-protection/consultative-committee-tpd/meetings abrufbar.

Seit der 47. Plenarsitzung wird die Vertretung durch das Bundesministerium für Justiz, Stabsstelle für Datenschutz, wahrgenommen.

43 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013R0603.

7. Internationale Beziehungen

Auch im Jahr 2024 fand wieder die Konferenz der Internationalen Datenschutzversammlung (**Global Privacy Assembly - GPA**)[44] statt. Die GPA ist seit mehr als vier Jahrzehnten ein wichtiges globales Forum für Aufsichtsbehörde im Datenschutzbereich.

Die diesjährige Global Privacy Assembly wurde von der Aufsichtsbehörde von Jersey vom 28. Oktober bis 1. November 2024 auf der **Kanalinsel Jersey** im hybriden Rahmen abgehalten, wobei vom 28. bis 30. Oktober 2024 die offene und vom 31. Oktober bis 1. November 2024 die geschlossene Sitzung stattfanden.

Die Vorträge und Diskussionen der offenen Sitzung konzentrierten sich auf aktuelle technologische Innovationen und deren Einfluss auf die Menschheit im Allgemeinen und auf Individuen im Besonderen. Besonderes Augenmerk wurde auf vulnerable Gruppen, wie etwa Jugendliche oder ältere Menschen sowie indigene Bevölkerungsgruppen, gelegt. Ebenso wurden Herausforderungen bei der weltweiten Durchsetzung von datenschutzrechtlichen Standards sowie die diesbezügliche Rolle der Datenschutzaufsichtsbehörden thematisiert.

Am Ende der offenen Sitzung wurde, nunmehr zu vierten Mal, der „**Giovanni Buttarelli Award“** verliehen, der 2024 an den ehemaligen Leiter der Abteilung in der Europäischen Kommission für Datenschutz und internationale Datenflüsse, Bruno Gencarelli, ging.[45]

In der geschlossenen Sitzung erstatteten die GPA-Arbeitsgruppen und verschiedene GPA-Mitglieder und Beobachter:innen sowie die Berliner Gruppe und andere Partnerorganisationen der Versammlung ihre Tätigkeitsberichte. Darüber hinaus wurden die folgenden **Resolutionen**[46] angenommen:

- Resolution zur verstärkten Nutzung von Datenschutz-Zertifizierungsmechanismen;
- Resolution zu den Grundsätzen der Verarbeitung personenbezogener Daten im Rahmen der Neurowissenschaft und Neurotechnologie;
- Resolution zu vertrauensvollen Datenflüssen und einer effektiven Regulierung grenzüberschreitender Datenströme; und
- Resolution zur Geschäftsordnung der GPA.

Die Datenschutzaufsichtsbehörde von **Südkorea** wird die GPA im Jahr 2025 ausrichten.

7.1. Bilaterale Kooperationen mit Datenschutz-Aufsichtsbehörden

Die mit 1. Jänner 2024 neu bestellte Leitung hat als einen ihrer Schwerpunkte für die künftige Arbeit der DSB die verstärkte grenzüberschreitende Kooperation gesetzt.[47] Der Fokus wurde zunächst auf die **Datenschutzaufsichtsbehörden der unmittelbaren Nachbarländer** gelegt.

44 Siehe hierzu https://gpajersey.com/.
45 Siehe hierzu https://globalprivacyassembly.org/news-events/giovannibuttarelliaward/.
46 Siehe hierzu https://globalprivacyassembly.org/document-archive/adopted-resolutions/.
47 Siehe hierzu den Eröffnungsbeitrag im DSB-Newsletter 1/2024, abrufbar unter https://dsb.gv.at/sites/

Bereits Anfang des Jahres 2024, am 19. und 20. Februar, fand ein Treffen zwischen der DSB und dem **damaligen deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)**, Prof. Ulrich Kelber, sowie mit dem **Bayerischen Landesbeauftragten für den Datenschutz (BayLfD)**, Prof. Thomas Petri, in Wien statt. Die DSB hat den gegenseitigen Austausch genutzt, um zahlreiche Themen, welche aktuell den EDSA beschäftigen, zu erörtern und die bi- und multilaterale Kooperation mit dem BfDI und dem BayLfD zu fördern. Darüber hinaus wurden organisatorische Aspekte der grenzüberschreitenden Verfahrensführung und der Zusammenarbeit mit deutschen Datenschutz-Aufsichtsbehörden besprochen.

Der BfDI und der BayLfD übernehmen im innerdeutschen Gefüge Schlüsselaufgaben in Bezug auf die nationale Abstimmung der deutschen Datenschutz-Aufsichtsbehörden, die im Rahmen der Datenschutzkonferenz erfolgt. Dort erfolgt im Wesentlichen mittels Entschließungen, Beschlüssen, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen eine Verständigung auf eine gemeinsame deutsche Position der Datenschutz-Aufsichtsbehörden aller deutscher Bundesländer.[48]

Im Sommer 2024 hat Prof. Louisa Specht-Riemenschneider das Amt der BfDI übernommen.

Im Juni 2024 besuchte die Leitung der DSB den **Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)** in Bern. Primäres Ziel war ein Erfahrungsaustausch im Hinblick auf die Informationsfreiheit (Näheres siehe in **Kapitel 3.1.**). Auch wenn die Schweiz nicht dem EWR angehört, ist eine bilaterale Zusammenarbeit mit dem EDÖB von Bedeutung, wie etwa bei der Behandlung von grenzüberschreitenden Fällen gegen Verantwortliche mit Sitz in der Schweiz. Den diesbezüglichen Rechtsrahmen bildet das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[49], welches sowohl von Österreich als auch von der Schweiz ratifiziert wurde und in seinen Art. 13 ff Bestimmungen über die gegenseitige Hilfeleistung zwischen Behörden enthält.

Den Höhepunkt der bilateralen Kooperation der DSB im Jahr 2024 bildete ein Treffen mit den Datenschutzaufsichtsbehörden von **Tschechien, Ungarn, Slowenien und der Slowakei** in Wien, welches am 12. und 13. September 2024 in den Räumlichkeiten der DSB abgehalten wurde. Auch dieses Treffen hatte das Ziel, den gegenseitigen Austausch und Zusammenarbeit auf nationaler und europäischer Ebene unter Wahrung der eigenen Unabhängigkeit zu verfestigen.

Thematisch wurde ein breiter Bogen gespannt. Hervorzuheben sind hier insbesondere Fragen zur Informationsfreiheit. Da die Datenschutz-Aufsichtsbehörden von Tschechien, Ungarn und Slowenien bereits seit Langem auch Kompetenzen im Bereich der Informationsfreiheit ha-

site0344/media/downloads/newsletter_dsb_1_2024_1.pdf.

48 In Deutschland wurde – anders als in Österreich – für jedes Bundesland eine eigene Datenschutz-Aufsichtsbehörde geschaffen (in Bayern bestehen zwei Aufsichtsbehörden mit unterschiedlichem Kompetenzbereich). Darüber hinaus wurde mit dem BfDI eine Aufsichtsbehörde auf Bundesebene eingerichtet. Im Europäischen Datenschutzausschuss, welchem Aufsichtsbehörden aller EU-Mitgliedstaaten sowie der Länder Island, Liechtenstein und Norwegen und der Europäische Datenschutzbeauftragte angehören, hat jedes Mitglied nur eine Stimme. Da in Deutschland mehrere Aufsichtsbehörden eingerichtet sind, ist gemäß § 17 dBDSG ein gemeinsamer Vertreter und eine zentrale Anlaufstelle eingerichtet. Diese Funktion kommt ex lege der BfDI zu. Die Stellvertretung obliegt dem Ländervertreter, dessen Hauptaufgabe insbesondere in der Ermittlung und Abstimmung des innerdeutschen Standpunktes im Vorfeld der Plenarsitzungen des Europäischen Datenschutzausschusses besteht. Dem Ländervertreter obliegt die Abstimmung für Deutschland im Europäischen Datenschutzausschuss nicht nur im Verhinderungsfall der BfDI. Ihm sind in bestimmten wichtigen Angelegenheiten, welche die deutschen Bundesländer betreffen, auf Verlangen die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss zu übertragen. Der Ländervertreter wird vom deutschen Bundesrat auf fünf Jahre gewählt und die Funktion des Ländervertreters wird derzeit vom BayLfD ausgeübt.

49 BGBl. Nr. 317/1988 idgF. (Datenschutzkonvention 108).

ben, konnten hier wertvolle Erfahrungen gesammelt und ausgetauscht werden. Einen zweiten Schwerpunkt bildeten Fragen, mit denen sich Datenschutz-Aufsichtsbehörden im Rahmen der neuen EU-Digitalrechtsakte zu befassen haben (siehe Kapitel 3.4. und 3.5.).

Da die Datenschutz-Aufsichtsbehörden in Tschechien, Ungarn, Slowenien und der Slowakei eine ähnliche Größe und Struktur wie die DSB aufweisen und sich mit ähnlichen Herausforderungen konfrontiert sehen, wurden zahlreiche Überschneidungspunkte für eine verstärkte Zusammenarbeit ermittelt und ein regelmäßiger Austausch zu aktuellen Themen vereinbart. Ferner wurde beschlossen, das Treffen auf hochrangiger Ebene zu institutionalisieren und mindestens einmal im Jahr abzuhalten, wobei sich die ungarische Aufsichtsbehörde bereit erklärt hat, das nächste Treffen im Jahr 2025 in Budapest zu organisieren.

7.2. Teilnahme an TAIEX-Projekten[50]

TAIEX steht für „Technical Assistance and Information Exchange Instrument" („Informationsaustausch und technische Unterstützung") und ist ein überwiegend nachfragegesteuertes Instrument der Europäischen Kommission. TAIEX unterstützt öffentliche Verwaltungen im Hinblick auf die Annäherung, Anwendung und Umsetzung europäischer Rechtsakte und stellt kurzfristig maßgeschneidertes Expertenwissen zur Verfügung. Zu den Serviceleistungen gehören kurzfristige technischen Beratungen und Schulungen (Workshops, Expertenvorträge) und Studienbesuche.

Der Fokus der DSB lag im Jahr 2024 auf der Unterstützung der **kosovarischen Datenschutzaufsichtsbehörde**, welcher im Oktober 2024 der Beobachterstatus im Europäischen Datenschutzausschuss zuerkannt wurde.[51]

Die DSB wurde für Mai 2024 von der Europäischen Kommission für eine TAIEX-Mission (*„TAIEX Expert Mission on data protection and investigations in the law enforcement sector"*) bei der kosovarischen Aufsichtsbehörde („Information and Privacy Agency of Kosovo") in Prishtina nominiert.

Die entsandten Mitarbeiter:innen der österreichischen DSB haben bei der kosovarischen DSB in Prishtina intensive Schulungen und Beratungen zu datenschutzrechtlichen Aspekten bei der Verarbeitung personenbezogener Daten durch Polizei- und Sicherheitsbehörden[52] in englischer Sprache praxisnahe durchgeführt. Dabei konnten die österreichischen Vertreterinnen sich auch Einblick in das bereits vorhandene, sehr hohe Niveau der kosovarischen Aufsichtsbehörde in Bezug auf das Datenschutzrecht verschaffen, welche oftmals ähnliche praktische und rechtliche Problemstellungen zu lösen hat, wie die DSB.

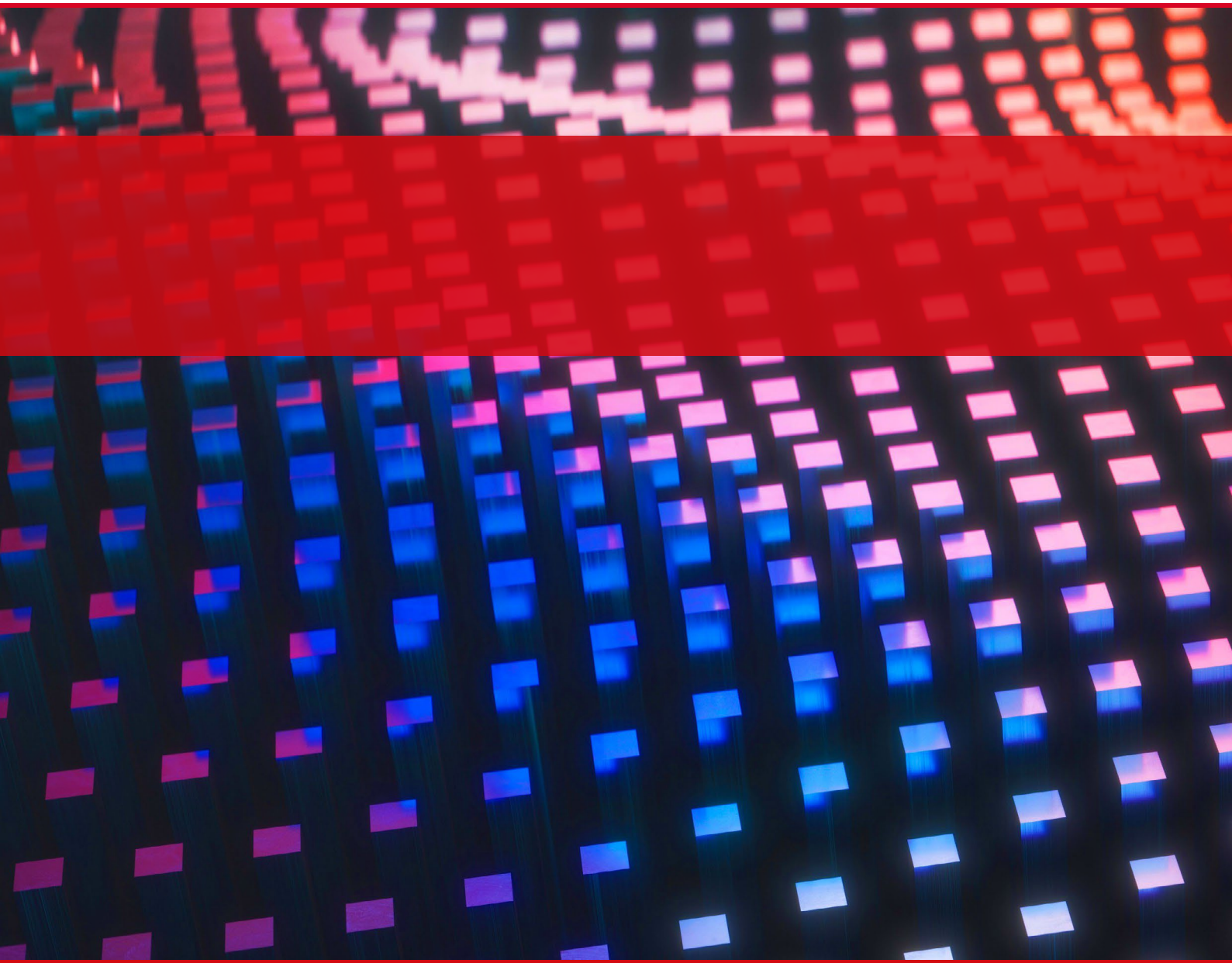
Bei einem darauf aufbauenden dreitägigen TAIEX-Studienbesuch der kosovarischen Datenschutzaufsichtsbehörde im Dezember 2024 in Wien (*„TAIEX Study Visit on the implementation of the Law for the Personal Data Protection in Specific Fields/Case Studies"*) stellte die DSB ihre Struktur und Arbeitsweise vor. Der Fokus wurde auf nahezu alle Tätigkeitsfelder der DSB gelegt

50 https://neighbourhood-enlargement.ec.europa.eu/funding-and-technical-assistance/taiex_en.

51 Siehe hierzu Punkt B.4. des Protokolls zur 97. Sitzung des Europäischen Datenschutzausschusses vom 7. und 8. Oktober 2024, abrufbar in englischer Sprache unter https://www.edpb.europa.eu/system/files/2024-11/20241007-08plenfinalminutes97thplenary_en_0.pdf.

52 D.h. im Anwendungsbereich der RL (EU) 2016/680.

und wurden der Verfahrensgang von nationalen Beschwerde- und Prüfverfahren, grenzüberschreitenden Verfahren und Verwaltungsstrafverfahren sowie sich daraus ergebende Fragen umfassend erörtert. Ferner wurden (im Bedarfsfall entsprechend anonymisierte) Fallbesprechungen aus den Bereichen Gesundheitsdaten (inklusive Vorstellung des öst. Gesundheitstelematikgesetzes und der elektronischen Gesundheitsakte), Datenschutz-Folgenabschätzung am Beispiel des österreichischen E-Government Systems, und „Leuchtturmfälle“ wie der Jö Bonus Club und Google Analytics präsentiert.



	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-04-29T10:05:32+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	