dsb

Republik Österreich

Datenschutz behörde

Tätigkeitsbericht 2025

- Datenschutz
- Informationsfreiheit
- Künstliche Intelligenz
- Transparenz und Targeting in der politischen Werbung
- Plattformarbeit

www.dsb.gv.at

dsb@dsb.gv.at

Tätigkeitsbericht 2025

Wien, im März 2026

Republik Österreich
Datenschutz
behörde

Impressum

Medieninhaber, Herausgeber und Redaktion:
Datenschutzbehörde, Dr. Matthias Schmidl
(gemäß § 18ff 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, 2026

Abkürzungsverzeichnis

ABl.	Ausschussbericht
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
ArbVG	Arbeitsverfassungsgesetz
Art.	Artikel
ÄrzteG	ÄrzteGesetz 1998
ASVG	Allgemeines Sozialversicherungsgesetz
BGBl.	Bundesgesetzblatt
BMJ	Bundesministerium für Justiz
bspw.	beispielsweise
B-VG	Bundes-Verfassungsgesetz
BVwG	Bundesverwaltungsgericht
BVwGG	Bundesverwaltungsgerichtsgesetz
bzw.	beziehungsweise
dh.	das heißt
DMA	Digital Markets Act
DSB	Datenschutzbehörde
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EU-GRC	Charta der Grundrechte der Europäischen Union
EWR	Europäischer Wirtschaftsraum
FMA	Finanzmarktaufsicht
FM-GwG	Finanzmarkt-Geldwäschegesetz
FN	Fußnote
GPA	Global Privacy Assembly
GTelG	Gesundheitstelematikgesetz 2012
IFG	Informationsfreiheitsgesetz
IO	Insolvenzordnung
iSd.	im Sinne der/des
iVm.	in Verbindung mit
JN	Jurisdiktionsnorm
KI	Künstliche Intelligenz
KI-VO	Verordnung über Künstliche Intelligenz
KSchG	Konsumentenschutzgesetz
lit.	litera (-ae)
LG	Landesgericht
LVwG	Landesverwaltungsgericht
mwN	mit weiteren Nachweisen

• Nr.	Nummer
• ORF	Österreichischer Rundfunk
• ORF Beitragsgesetz 2024	ORF-Beitrags-Gesetz 2024
• ORF-G	ORF-Gesetz
• PartG	Parteiengesetz
• PDK	Parlamentarisches Datenschutzkommitee
• RIS	Rechtsinformationssystem
• Rz.	Randziffer
• SIS	Schengener Informationssystem
• TKG 2021	Telekommunikationsgesetz 2021
• VfGG	Verfassungsgerichtshofgesetz 1953
• VfGH	Verfassungsgerichtshof
• VfSlg.	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des Verfassungsgerichtshofes
• vgl.	vergleiche
• VGW	Verwaltungsgericht Wien
• VIS	Visa-Informationssystem
• VStG	Verwaltungsstrafgesetz 1991
• VwGH	Verwaltungsgerichtshof
• VwSlg.	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des Verwaltungsgerichtshofes
• Web-ERV	Webbasierter elektronischer Rechtsverkehr
• WiEReG	Register der wirtschaftlichen Eigentümer
• Z	Ziffer
• zB.	zum Beispiel
• ZIS	Zoll Informations System
• ZMR	Zentrales Melderegister

1. Vorwort

Sehr geehrte Leserinnen und Leser!

Wie Sie dem Umschlag bereits entnehmen können, legt die Datenschutzbehörde in diesem Jahr keinen Datenschutzbericht, sondern einen **Tätigkeitsbericht für das Jahr 2025** vor.

Das entspricht zum einen der Vorgabe des § 23 Abs. 1 DSG, der von einem Tätigkeitsbericht spricht.

Der andere, jedoch ausschlaggebende Grund liegt darin, dass die DSB seit 2025 nicht mehr bloß Aufgaben nach der DSGVO und dem DSG wahrnimmt, sondern weitere Aufgaben hinzugekommen sind.

In erster Linie ist hier das **IFG** zu erwähnen, das in **§ 15** der DSB eine Sonderrolle zuweist. Sie hat die informationspflichtigen Organe durch die Bereitstellung eines Leitfadens zu beraten, Schulungen anzubieten und das IFG begleitend zu evaluieren.

Wie im Datenschutzbericht 2024 bereits erwähnt, sehen mehrere Unionsrechtsakte zusätzliche Aufgaben für die DSB außerhalb ihres angestammten Vollzugsbereiches vor: Die **Verordnung über künstliche Intelligenz (KI-VO)**, die V**erordnung über die Transparenz und das Targeting politischer Werbung**, die **NIS 2-Richtlinie** und die **Richtlinie über Plattformarbeit** sind als die wichtigsten zu nennen. In diesem Zusammenhang zu erwähnen ist auch die **Datenverordnung (Data Act)**, die derzeit im Rahmen der **„Digitale-Omnibus-Verordnung"** umfassend novelliert werden soll.

Diese Unionsrechtsakte, deren Umsetzung bzw. Durchführung vor allem das Jahr 2026 bestimmen wird, haben die Tätigkeit der DSB bereits im Jahr 2025 maßgeblich beeinflusst, weil für diese neuen Aufgaben umfassende Vorbereitungen notwendig sind.

Die Umstellung der Bezeichnung von „Datenschutzbericht" auf „Tätigkeitsbericht" soll daher schon im Titel zum Ausdruck bringen, dass die DSB weitere Aufgaben wahrzunehmen hat, die zwar auch mit der Verarbeitung personenbezogener Daten im Zusammenhang stehen (können), der Vollzug jedoch nicht auf Basis der DSGVO, sondern anderer Rechtsakte erfolgt.

Das Berichtjahr 2025 war für die DSB ein sehr herausforderndes: Es stand ganz im Zeichen eines **restriktiven Budgetvollzugs auf Bundesebene**. Wie viele andere Bundesbehörden auch, verzeichnet die DSB **Budgetkürzungen**, die sich wiederum auf die Tätigkeit der DSB auswirken, da die zur Verfügung stehenden Mittel für Verwaltungspraktikantinnen und -praktikanten signifikant gekürzt werden. Die DSB hat darüber im **Newsletter 2/2025** ausführlich berichtet und auch der vorliegende Bericht wird sich dieser Thematik eingehend widmen.

Erschwerend kommt hinzu, dass vor allem im Bereich der **Beschwerdeverfahren** (sowohl national auch als auch grenzüberschreitend) eine **deutliche Steigerung der Verfahrenseingänge** festzustellen war. Gleichzeitig zeigen die Zahlen, dass die von der DSB ergriffenen Maßnahmen (vor allem die so genannten Erstsichtungen) greifen und so zu einer – teilweisen – Entlastungen der Bediensteten beitragen.

Trotz dieser Herausforderungen ist es der DSB überwiegend gelungen, ihren Aufgaben nachzukommen und vor allem **Verfahren in einem hohen Ausmaß zu beenden**.

Mein Dank gilt daher in erster Linie den Bediensteten der DSB, die unter den gegenwärtigen, schwierigen Bedingungen ausgezeichnete Arbeit leisten.

Um die Verfahrensführungen effizienter zu gestalten, erachtet die DSB eine **Novelle des DSG** als **erforderlich**. Erste Gespräche mit dem fachlich zuständigen BMJ haben bereits stattgefunden.

Am 19. November 2025 wurde darüber hinaus von der Europäischen Kommission der Vorschlag für eine so genannte **„Digitale-Omnibus-Verordnung"** vorgelegt, welche u.a. eine Novelle der DSGVO vorsieht. Diese Novelle kann durchaus als einschneidend bezeichnet werden, weil die Kommission darin weitreichende Änderungen der DSGVO, bspw. auch eine Neudefinition des Begriffs des personenbezogenen Datums, vorschlägt. Die DSB hat sich dazu im EDSA sowie in der innerstaatlichen Koordinierung bereits sehr intensiv eingebracht und wird dies auch im Jahr 2026 machen.

Daneben hat die DSB auf europäischer Ebene wie gewohnt **proaktiv im EDSA** mitgewirkt. Dieses Engagement wurde insofern belohnt, als ich von meinen Kolleginnen und Kollegen als eines von vier Mitgliedern des EDSA in die **Hochrangige Gruppe (High Level Group)** nach **Art. 40 des Gesetzes über Digitale Märkte (Digital Markets Act – DMA)** gewählt wurde und den EDSA in diesem Gremium „mitrepräsentieren" darf.

Die Zusammenarbeit mit den Aufsichtsbehörden unserer unmittelbaren Nachbarstaaten war auch im Berichtsjahr ein wesentliches Anliegen. Die von der DSB 2024 angestoßene engere **Kooperation mit den mitteleuropäischen Aufsichtsbehörden** aus Tschechien, der Slowakei, Ungarn, Slowenien und Kroatien wurde gleichsam institutionalisiert: Das erste Arbeitstreffen fand 2024 in Wien statt, im Jahr 2025 richtete die ungarische Aufsichtsbehörde das Treffen aus. Für das Jahr 2026 hat sich Slowenien bereit erklärt.

Im Berichtsjahr hat mit dem **PDK** die zweite Datenschutz-Aufsichtsbehörde in Österreich ihre Funktion aufgenommen. Die DSB hat das PDK in der Anfangsphase tatkräftig unterstützt, vor allem durch die Bereitstellung von Musterformularen für die Verfahrensführung, und pflegt einen regelmäßigen und vertrauensvollen Austausch mit dem PDK.

Die DSB hat ein herausforderndes Jahr 2025 hinter sich und blickt auf ein weiteres herausforderndes Jahr 2026, das richtungsweisende Änderungen bringen wird.

Es ist aus meiner Sicht sehr klar, dass ohne **zusätzliche budgetäre Mittel und personelle Aufstockung** die auf die DSB zukommenden Aufgaben nicht bewältigt werden können. Dies erfordert eine gesamtstaatliche Anstrengung und den Konsens der im Nationalrat vertretenen Parteien: Denn nur dort wird über das Bundesbudget und damit auch über die personelle Ausstattung der DSB entschieden. In Zeiten zunehmender Digitalisierung nimmt die DSB eine wesentliche Rolle ein, nämlich die einer Behörde, bei deren Vollzug der **Grundrechtsschutz** – und damit die **humanistische Komponente** – im Vordergrund steht.

Digitalisierung ist kein Selbstzweck. Sie soll dem Menschen dienen und ihn nicht zum Objekt machen.

Ich wünsche Ihnen eine abwechslungsreiche und spannende Lektüre.
Dr. Matthias Schmidl, Leiter der DSB

2. Die Datenschutzbehörde

2.1 Organisation und Aufgaben

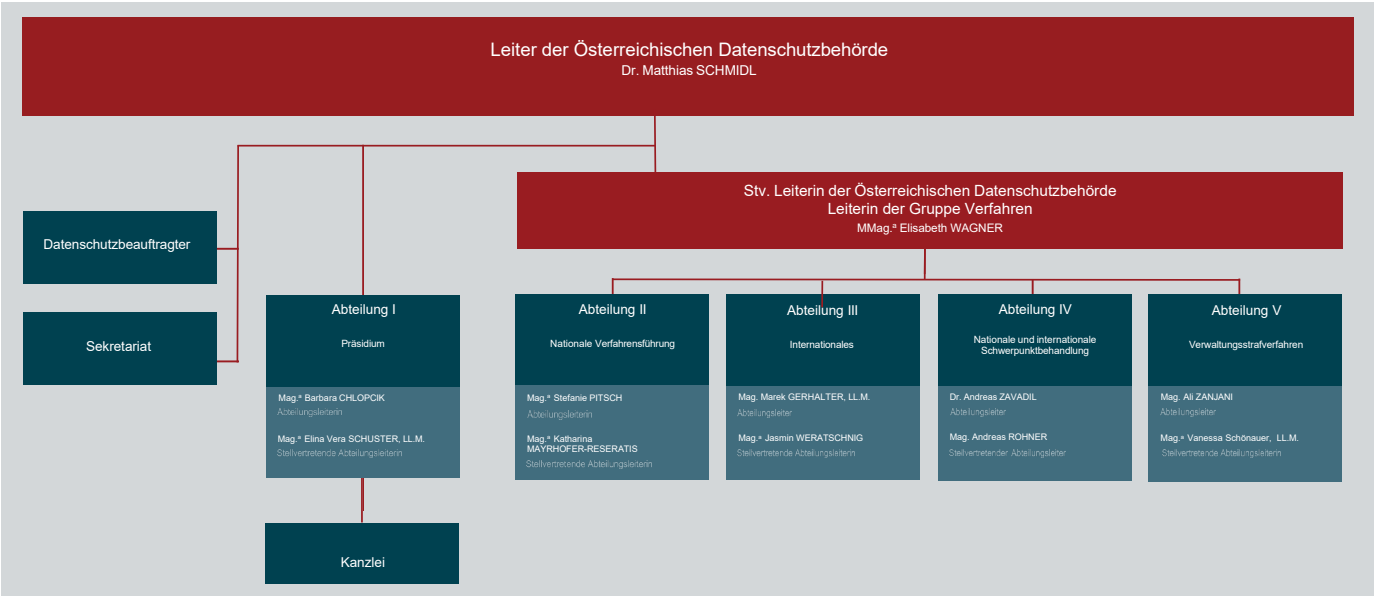
2.1.1 Organisation der Datenschutzbehörde

Die DSB ist **monokratisch** strukturiert, aufgrund europäischer und völkerrechtlicher Vorgaben **völlig unabhänig und keinder Dienst- und Fachaufsicht unterworfen**. Die Funktion des Leiters wird seit 1. Jänner 2024 von **Dr. Matthias Schmidl**, jene der stellvertretenden Leiterin von **MMag.a 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: Februar 2026



Die Abteilungsleiterinnen und –leiter 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 jeder:jede 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 dass Verwaltungsstrafverfahren somit unvoreingenommen geführt werden können.

2.1.2 Aufgaben und Befugnisse nach der DSGVO und dem DSG

Die **Aufgaben der DSB** sind vorrangig 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 allgemeine 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 Vermerk 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 ABl. Nr. L 2024/1689 vom 12. Juli 2024 kundgemacht und wird in den Folgejahren schrittweise in Geltung treten.

Vereits 2024 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 über die Transparenz und das Targeting politischer Werbung (Verordnung (EU) 2024/900)** wurde im ABl. kundgemacht (ABl. Nr. L 2024/900 vom 30. März 2024) und gilt seit 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.

2.1.6 Aufgaben nach der Richtlinie zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit

Diese **Richtlinie (Richtlinie (EU) 2024/2831)** wurde am 11. November 2024 im Amtsblatt kundgemacht (ABl. Nr. L 2024/2831 und ist bis 2. Dezember 2026 von den Mitgliedstaaten umzusetzen. Auch mit diesem Unionsrechtsakt werden den Datenschutz-Aufsichtsbehörden punktuell Zusatzaufgaben übertragen. Näheres wird in den **Kapiteln 3.3. und 11.** beschrieben.

2.2 Personalstand

Ende des Jahres 2025 umfasste der Personalstand der DSB insgesamt **58 Bedienstete**. Die Belegschaft setzte sich hierbei aus **34 weiblichen** und **24 männlichen** Bediensteten zusammen. Das Durchschnittsalter über alle Beschäftigtengruppen hinweg lag bei **38,8 Jahren**.

Das Personal der DSB teilte sich im Konkreten auf in:

- 43 Vertragsbedienstete (davon 3 besetzte Stellen gemäß Behinderteneinstellungsgesetz)
- 6 Beamt:innen
- 5 Verwaltungspraktikant:innen
- 4 Leiharbeitskräfte

Hinsichtlich der Entlohnungs- bzw. Verwendungsgruppen und der damit verbundenen Qualifikationsprofile ergab dies folgende Gliederung:

- A1 bzw. v1 (Höherer Dienst): 35 Personen
- A2 bzw. v2 (Gehobener Dienst): 14 Personen
- A3 bzw. v3 (Fachdienst): 9 Personen

Der Großteil der Zu- und Abgänge im Jahr 2025 entfiel auf den planmäßigen Wechsel der Verwaltungspraktikant:innen. Die Neubesetzung der Leitung und stellvertretenden Leitung der Abteilung II (Nationale Verfahren) bildete die wesentlichste personelle Veränderung im Berichtsjahr.

3. Wesentliche Ereignisse im Berichtsjahr sowie Ausblick auf die Folgejahre

Im Vordergrund stand im Jahr 2025 die **Wahrnehmung der der DSB übertragenen Aufgaben bei gleichzeitig restriktiven Budgetvollzug**. Weitere bestimmende Themen waren das IFG sowie die **KI-VO**.

Auf jene Themen, die die DSB im Berichtszeitraum stark beschäftigt bzw. beansprucht haben, wird in weiterer Folge im Detail eingegangen.

3.1 Personelle und budgetäre Entwicklung

Die DSB hat darüber im **Newsletter 2/2025**[1] ausführlich berichtet.

Hier sollen noch einmal die Eckdaten wiedergegeben werden:

- Das **Budget** für das Jahr 2024 betrug 5,7 Millionen Euro. Im Jahr 2025 beträgt das Budget der DSB 6,1 Millionen Euro, im Jahr 2026 wird es 5,9 Millionen Euro betragen.

- Der **Personalstand** der DSB (51 VBÄ[2]) bleibt unverändert, was dem großen Einsatz der Bundesministerin für Justiz zu verdanken ist.

- **Kürzungen** erfolgen insbesondere im Bereich der **Sachaufwendungen**. Dies hat zur Folge, dass die DSB seit Juli 2025, einen Großteil ihrer Verwaltungspraktikantinnen und –praktikanten (2025: rund 20 in Voll- und Teilzeit) nicht nachbesetzen kann.

- Durch Zusammenarbeit mit dem BMJ ist es gelungen, durch Sondermaßnahmen bzw. Umschichtung von Budgetmitteln diesen Personalabgang abzumildern.

- Die DSB sieht sich aufgrund dieser Entwicklungen gezwungen, klare **Schwergewichtsbildungen** vorzunehmen.

- Das **Schwergewicht Nummer 1** liegt in der **Behandlung von Beschwerden**, da hier eine Behandlungspflicht besteht und betroffene Personen ein subjektives Recht auf Behandlung ihrer Beschwerde haben. Verzögerungen in der Behandlung sind jedoch unvermeidlich.

- **Amtswegige Prüfverfahren** werden (in sinngemäßer Anwendung von § 45 VStG) nur mehr eingeleitet, wenn aus der Eingabe ein hinreichend konkreter Verdacht auf eine schwerwiegende Verletzung der DSGVO bzw. des DSG hervorgeht, wobei schützenswerten Gruppen (bspw. Kinder, Arbeitsnehmerinnen und –nehmer) besondere Beachtung eingeräumt wird. Es wird vermehrt von Sensibilisierungsschreiben Gebrauch gemacht werden.

1 Siehe nochmals https://dsb.gv.at/sites/site0344/media/downloads/newsletter_2_final.pdf.
2 Hier ist der Vollbeschäftigtenanteil im Jahr 2025 gemeint.

- **Jährliche Schwerpunktprüfungen**: Ankündigung des (jährlichen) Prüfungsschwerpunktes (Thema: etwa Datensicherheit) im Sinne einer Jahresstrategie ohne Bekanntgabe der Branche im Jänner jeden Jahres bei gleichzeitiger Bekanntgabe des tatsächlichen Starts der Prüfung (etwa im Mai).

- **Meldungen nach Art. 33 DSGVO** werden inhaltlich gesichtet. Allerdings ergeht eine Mitteilung an den Verantwortlichen nur mehr dann, wenn die DSB die Ansicht vertritt, dass Folgemaßnahmen erforderlich sind oder die Meldung unvollständig ist.[3]

- Die **telefonische Erreichbarkeit** wird **eingeschränkt** auf Mo bis Mi und Fr von 09:00 bis 12:00 und Do von 13:00 bis 15:30.

- **Schriftliche Rechtsauskünfte** werden nur mehr mit einem Verweis auf die ausführlichen Informationen auf der Webseite der DSB beantwortet.

- Die **Teilnahme von Bediensteten der DSB an Veranstaltungen**, auch als Vortragende, wird eingeschränkt.

- Die DSB wird an **Sitzungen der Untergruppen des EDSA** nur mehr dann teilnehmen, wenn das behandelte Thema ein wesentliches Interesse der DSB berührt.

- **Dienstreisen** werden auf das unbedingt notwendige Ausmaß reduziert.

- **Stellungnahmen im Gesetzes- und Verordnungsbegutachtungsverfahren** erfolgen nur mehr dann, wenn das Vorhaben grundsätzliche Fragen des Datenschutzes berührt.

Diese Entwicklungen und Maßnahmen waren auch Gegenstand der Behandlung des Datenschutzberichts 2024 im **Justizausschuss des Nationalrates am 30. September 2025**, zu dem der Leiter der DSB als Auskunftsperson geladen wurde.[4] Die Arbeit der DSB wurde fraktionsübergreifend von allen Abgeordneten gewürdigt, was zeigt, dass die Arbeit der DSB geschätzt wird.

3.2 Zusatzaufgaben der DSB

Auf diese Punkte wird im Detail in den **Kapiteln 8. bis 11.** eingegangen werden.

Dabei handelt es sich um:

- die **KI-VO**

- die **Verordnung über die Transparenz und das Targeting in der politischen Werbung**

- das **IFG** sowie

3 Siehe nochmals https://dsb.gv.at/sites/site0344/media/downloads/newsletter_2_final.pdf.
4 Siehe Parlamentskorrespondenz Nr. 824 vom 30.09.2025, https://www.parlament.gv.at/aktuelles/pk/jahr_2025/pk0824.

- die **Richtlinie über Plattformarbeit**

Die Vorbereitung auf diese Zusatzaufgaben bzw. deren Wahrnehmung nehmen erhebliche Ressourcen der DSB in Anspruch.

Ohne zusätzliches Personal – insbesondere mit technischer Ausbildung – werden diese Zusatzaufgaben nicht wahrgenommen werden können.

3.3 Omnibus-Pakete zur DSGVO

3.3.1 Digitale-Omnibus-Verordnung[5]

Eine Omnibus-Verordnung auf europäischer Ebene meint einen Gesetzesvorschlag, mit dem mehrere Gesetze (Verordnungen) geändert werden sollen. Dies entspricht einer Sammelnovelle in Österreich.

Der Vorschlag für eine Digitale-Omnibus-Verordnung sieht u.a. eine **bedeutsame Novelle der DSGVO** vor.

Die DSB hat die wesentlichsten Eckpunkte dieses Vorschlags bereits im **Newsletter 3/2025**[6] dargestellt:

- Änderung der Definition des Begriffs des „personenbezogenen Datums“ in Art. 4 Z 1 DSGVO dahingehend, dass eine natürliche Person für eine Stelle dann nicht als identifizierbar gilt, wenn diese Stelle die betroffene Person nicht identifizieren kann.;

- Ergänzung des Prinzips der Zweckbindung in Art. 5 Abs. 1 lit. b DSGVO, dahingehend, dass in bestimmten Fällen kein Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO durchzuführen ist.;

- Ergänzung von Art. 9 Abs. 2 DSGVO dahingehend, dass sensible Daten für Zwecke der Entwicklung und des Betriebs eines KI-Systems oder -Modells verarbeitet werden können.;

- Änderung von Art. 12 Abs. 5 DSGVO dahingehend, dass einem Auskunftsbegehren nicht entsprochen werden muss oder eine Gebühr verlangt werden kann, wenn damit datenschutzfremde Zwecke verfolgt werden.;

- Ergänzung von Art. 13 DSGVO dahingehend, dass die Information nicht zu erteilen ist, wenn aufgrund der Umstände der Datenerhebung klar ist, welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden.;

5 Siehe Proposal for a Regulation of the European Parliament and the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final, abrufbar unter https://digital-strategy.ec.europa.eu/de/library/digital-omnibus-regulation-proposal.

6 https://dsb.gv.at/sites/site0344/media/downloads/dsb-newsletter_nr._03_25_dezember_2025.pdf, abgerufen am 17.02.2026.

- Änderung von Art. 33 DSGVO dahingehend, dass für eine Meldung an die Aufsichtsbehörde auf ein hohes Risiko (wie in Art. 34 DSGVO) abgestellt und die Meldefrist auf 96 Stunden erhöht wird.;

- Änderung von Art. 33 DSGVO dahingehend, dass künftig die Meldungen über ein einheitliches Portal erfolgen können und der Europäische Datenschutzausschuss ein einheitliches Meldeformular entwickeln soll.;

- Änderung von Art. 35 DSGVO dahingehend, dass der Ausschuss eine Liste jener Verarbeitungstätigkeiten, für welche eine DSFA (nicht) durchzuführen ist, erstellen und an die Kommission übermitteln soll, die dann einen Durchführungsrechtsakt erlässt.;

- Einfügung eines Art. 88a, wonach Datenverarbeitungen auf Endgeräten in den Anwendungsbereich der DSGVO fallen sollen (bisher: RL 2002/58/EG);

- Einfügung eines Art. 88b, der das so genannte „Cookie-Management" neu regelt (mit einer Ausnahme für Medienunternehmen).;

- Einfügung eines Art. 88c, wonach die Verarbeitung personenbezogener Daten für das Entwickeln oder den Betrieb eines KI-Systems bzw. eines -Modells ein berechtigtes Interesse iSd Art. 6 Abs. 1 lit. f DSGVO darstellen kann.

Die DSB wird sich zu diesen Änderungsvorschlägen sowohl im Rahmen des **EDSA** (hier wurde bereits eine gemeinsame Stellungnahme mit dem Europäischen Datenschutzbeauftragten verabschiedet), als auch bei der Festlegung der **österreichischen Position im Rat** der Europäischen Union einbringen.

3.3.2 Digitale-Omnibus-Verordnung KI[7]

Mit diesem, ebenfalls am 19. November 2025 vorgestellten Vorschlag ist u.a. eine **Novelle der KI-VO** geplant.

Wesentliche Änderungen betreffen die Einfügung eines **Art. 4a**, mit welchem die **Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke der Erkennung von Verzerrungen und der Abhilfe ("bias detection and mitigation")** normiert werden soll, sowie die geplante Änderung von Art. 77, der die DSB als Grundrechtsbehörde betrifft.

3.4 Notwendigkeit einer Novelle des DSG

Die oben näher dargestellte Situation – zunehmende Anzahl an Aufgaben, steigende Verfahrenszahlen, sinkende Zahl an Bediensteten – hat die DSB dazu veranlasst, mit **konkreten Vorschlägen für eine Novelle des DSG** an das BMJ heranzutreten.

7 Proposal for a Regulation of the European Parliament and the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM(2025) 836 final, abrufbar unter https://digital-strategy.ec.europa.eu/de/library/digital-omnibus-ai-regulation-proposal.

Diese Vorschläge betreffen vor allem verfahrensrechtliche Bestimmungen, weil diese in die Autonomie der Mitgliedstaaten fallen.

Die Vorschläge der DSB zielen darauf ab, einerseits die **Verfahrensführung** zu **beschleunigen** sowie andererseits aber **punktuell längere Verjährungsfristen** vorzusehen, um Verfahren ordnungsgemäß führen zu können.

Eine erste inhaltliche Besprechung fand im Berichtszeitraum statt.

3.5 Missbräuchlich erhobene Beschwerden

Im Berichtsjahr konnte verstärkt festgestellt werden, dass Beschwerden oftmals in rechtsmissbräuchlicher Absicht erhoben werden. Davon ist – der Rechtsprechung des VwGH folgend – vor allem auszugehen, wenn der Beschwerde **kein genuines datenschutzrechtliches Interesse** zugrunde liegt, die Beschwerdeführung bspw. aus Gründen der Publicity oder Effekthascherei erfolgt oder das Anliegen vom Anwendungsbereich der DSGVO überhaupt nicht umfasst ist.

Im Fall von offenkundig rechtsmissbräuchlich erhobenen Beschwerden ist die DSB dazu übergegangen, den:die Beschwerdeführer:in auf die Rechtsmissbräuchlichkeit aufmerksam zu machen und eine **Ablehnung der Behandlung oder die Vorschreibung einer Gebühr gemäß Art. 57 Abs. 4 DSGVO** in Aussicht zu stellen, sofern keine nähere Begründung erfolgt, die den Verdacht der Rechtsmissbräuchlichkeit entkräftet. Dies bewirkt vielfach, dass solche Beschwerden zurückgezogen werden und somit personelle Ressourcen für jene Beschwerdefälle zur Verfügung stehen, denen ein genuines Rechtsschutzinteresse zugrunde liegt.

3.6 Mit Hilfe von KI erstellte Beschwerden

Ebenso konnte festgestellt werden, dass eine **Vielzahl von Beschwerden offenkundig unter Zuhilfenahme von Sprachmodellen** (Large Language Models – LLMs), dh. auf KI-Modellen basierende ChatBots wie ChatGPT u.a., erstellt werden. Erkennbar sind diese Beschwerde vor allem an ihrem Umfang sowie daran, dass ausdrücklich und gezielt auf einschlägige Bestimmungen der DSGVO Bezug genommen wird. Insofern unterscheiden sich solche Beschwerden schon von ihrer Struktur und ihrem Inhalt her von Beschwerden, die von einem:einer durchschnittlichen Beschwerdeführer:in eingebracht werden.

Auch dieses Phänomen, von dem im Übrigen auch viele andere Datenschutz-Aufsichtsbehörden der EU berichten, **binden erhebliche Ressourcen der DSB**.

3.7 Amtshaftungskosten

Das gestiegene Volumen an Beschwerden (national und grenzüberschreitend) bei real sinkenden Bedienstetenzahlen führte im Berichtszeitraum dazu, dass **vermehrt Schadenersatz aus dem Titel der Amtshaftung** zu leisten war.

Amtshaftungsansprüche werden v.a. dann geltend gemacht, wenn die DSB mit einer Entscheidung säumig ist und **Säumnisbeschwerde an das BVwG** erhoben wird. Die dabei anfallenden Kosten (Eingabegebühr, anwaltliche Kosten) können als Amtshaftungsansprüche geltend gemacht werden.

Im Berichtszeitraum hat die DSB **EUR 9.626,60,-** für anerkannte Amtshaftungsansprüche geleistet.

Diese Kosten belasten das Budget der DSB zusätzlich zu jenen Kosten, die die DSB zu tragen hat, weil das BVwG mit einer Entscheidung säumig ist (§ 47 Abs. 5 VwGG). Hier fielen im Berichtszeitraum Kosten in Höhe von **EUR 5.639,20,-** an.

3.8 Zusammenarbeit mit dem parlamentarischen Datenschutzkomitee - PDK

Das **PDK**[8] nahm am 1. Jänner 2025 seine Tätigkeit als zweite Datenschutz-Aufsichtsbehörde in Österreich auf. Im Gegensatz zur DSB ist das PDK eine **Kollegialbehörde**, bestehend aus bis zu sechs Mitgliedern mit jährlich rotierendem Vorsitz.

Der Vollzugsbereich des PDK umfasst die **Aufsicht über sämtliche Organe im Dienste der Gesetzgebung, einschließlich der ihnen zukommenden Verwaltungsaufgaben**, dh. im Wesentlichen **National- und Bundesrat, alle Landtage, (Landes-)Volksanwaltschaft(en) sowie Rechnungshöfe**.

Die Vollzugsbereiche der DSB und des PDK schließen sich wechselseitig aus.

Die Vertretung im EDSA obliegt dem Leiter der DSB, wobei das PDK einzubinden ist.

Im Berichtszeitraum fanden zahlreiche Treffen zwischen DSB und PDK statt. Einerseits, um einander besser kennenzulernen, andererseits aber auch, um wesentliche Informationen von beidseitigem Interesse auszutauschen.

8 Siehe https://pdk.gv.at/.

3.9 Netzwerk Digitalisierung

Im November 2024 wurde über maßgebliche Initiative der DSB die **„Erklärung über ein Netzwerk Digitalisierung“** unterzeichnet.

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 Dezember 2025 wurde beschlossen, auch das **PDK** aufzunehmen.

Im Fokus steht dabei der wechselseitige Informationsaustausch zu Themen der Digitalisierung (v.a. künstliche Intelligenz), da diese Themen alle Behörden gleichermaßen betreffen und Auswirkungen auf alle Lebensbereiche haben.

Im Berichtszeitraum fanden zwei Treffen auf Leitungsebene statt. Die DSB richtete darüber hinaus zwei Treffen aus (eines zum Thema Informationsfreiheit).

3.10 Beschwerden an die Volksanwaltschaft und andere Stellen

In **3 Fällen** wurde die DSB von der Volksanwaltschaft zur Stellungnahme aufgefordert, weil sich Beschwerdeführer:innen an sie gewendet hatten. Damit ist die Zahl im Vergleich zu den Vorjahren (2024: 10 Beschwerden, 2023: 21) erneut deutlich gesunken, wobei auch im Jahr 2025 zwei von drei Beschwerden vom selben Beschwerdeführer eingebracht wurden.

3.11 Parlamentarische Anfragen

Im Jahr 2025 wurden **keine** die DSB betreffenden parlamentarischen Anfragen an die Bundesministerin für Justiz gestellt.

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.

3.12 Informationsfreiheit

Im Berichtszeitraum war die DSB nicht nur mit der **Vorbereitung auf das IFG**, sondern auch mit **konkreten Informationsfreiheitsbegehren** befasst (siehe dazu Kapitel 10.). Die **erste Evaluierung** (§ 15 Abs. 2 IFG) ist ebenfalls diesem Tätigkeitsbericht zu entnehmen, wobei dabei ernsthafte Probleme auftraten. Da insbesondere keine gesetzliche Verpflichtung informationspflichtiger Stellen besteht, der DSB aussagekräftiges Datenmaterial, wie bspw. Anzahl der Informationsfreiheitsbegehren, Art der Entscheidung darüber etc., zur Verfügung zu stellen, ist die DSB im Wesentlichen auf das Wohlwollen informationspflichtiger Stellen angewiesen, was eine umfassende Evaluierung erheblich erschwert. Näheres kann **Kapitel 10.** entnommen werden.

4. Tätigkeit der Datenschutzbehörde

4.1 Statistische Darstellung

Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2023	2024	**2025**	2023	2024	**2025**
Beschwerden - Inland						
Individualbeschwerden	2389	3019	**5300**	1978	2397	**3403**
Erledigungsart der Individualbeschwerden				1485 Bescheide 493 Einstellungen	1845 Bescheide 552 Einstellungen	**2332** Bescheide **1071** Einstellungen
Beschwerden - Ausland						
Beschwerden grenzüberschreitend (im Ausland einlangend)	443	194	**173**	76	27	**32**
davon: Beschwerden grenzüberschreitend (im Ausland einlangend, One Stop Shop - Österreich betroffen) ***IMI:*** *Internal Market Information System*		175 (von insgesamt 856 über IMI eingelangten Meldungen)	**152** (von insgesamt 1207 über IMI eingelangten Meldungen)		17 Einstellungen	**22** Einstellungen
davon: Beschwerden grenzüberschreitend (im Ausland einlangend, O.S.S. - Österreich federführend)		19	**21**		3 Bescheide 7 Einstellungen	**1** Bescheid **9** Einstellungen

Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2023	2024	**2025**	2023	2024	**2025**
Beschwerden grenzüberschreitend (in Österreich einlangend)	433	600	**1364**	364	275	**760**
davon: Beschwerden grenzüberschreitend (in Österreich einlangend - Behandlung im O.S.S)		511	**1038**		96 Bescheide 147 Einstellungen	**297** Bescheide **290** Einstellungen
davon: Beschwerden grenzüberschreitend (in Österreich einlangend – Drittstaat, keine O.S.S. - Behandlung in Österreich)		89	**326**		9 Bescheide 23 Einstellungen	**105** Bescheide **68** Einstellungen

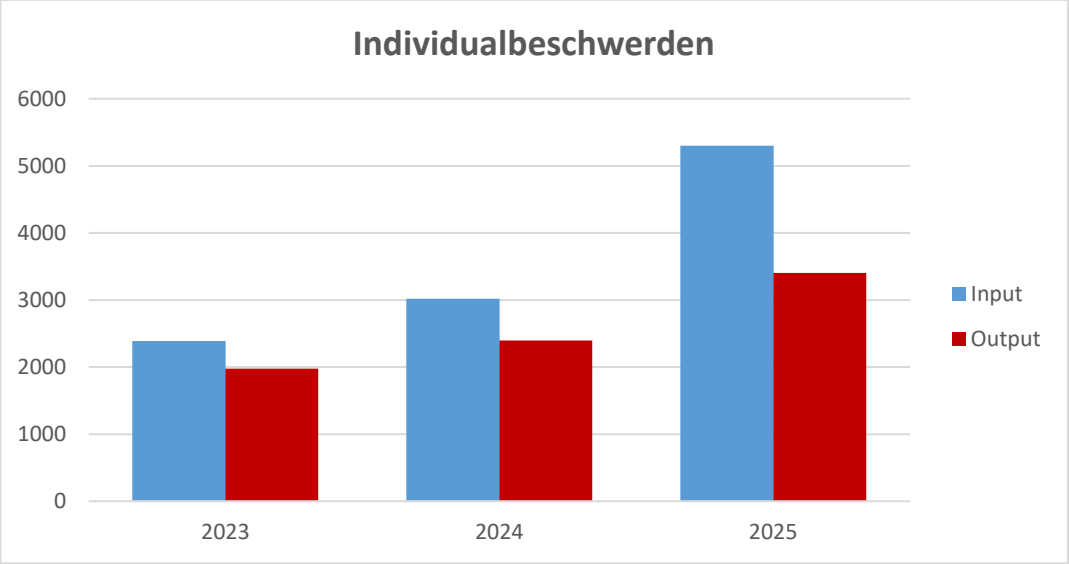
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2023	2024	**2025**	2023	2024	**2025**
AMTSWEGIGE PRÜFVERFAHREN						
Amtswegige Prüfverfahren	765	646	**225**	549	504	**222**
Erledigungsart der amtswegigen Prüfverfahren				12 Bescheide 537 Einstellungen	8 Bescheide 496 Einstellungen	**10** Bescheide **212** Einstellungen
VERWALTUNGSSTRAFVERFAHREN						
Verwaltungsstrafverfahren	176	211	**127**	196	214	**143**
Erledigungsart der Verwaltungsstrafverfahren				58 Bescheide 138 Einstellungen	62 Bescheide 152 Einstellungen	**58** Bescheide **85** Einstellungen
Erstsichtungen			**1800**			
SICHERHEITSVERLETZUNGEN						
Sicherheitsverletzungen gesamt	1142	1319	**1855**	786	936	**1804**
Sicherheitsverletzungen nach dem TKG 2021	28	55	**83**	19	36	**80**
Sicherheitsverletzungen Art. 33 DSGVO	1028	1216	**1704**	734	870	**1666**
Sicherheitsverletzungen grenzüberschreitend (in Österreich einlangend)	30	39	**48**	20	27	**46**

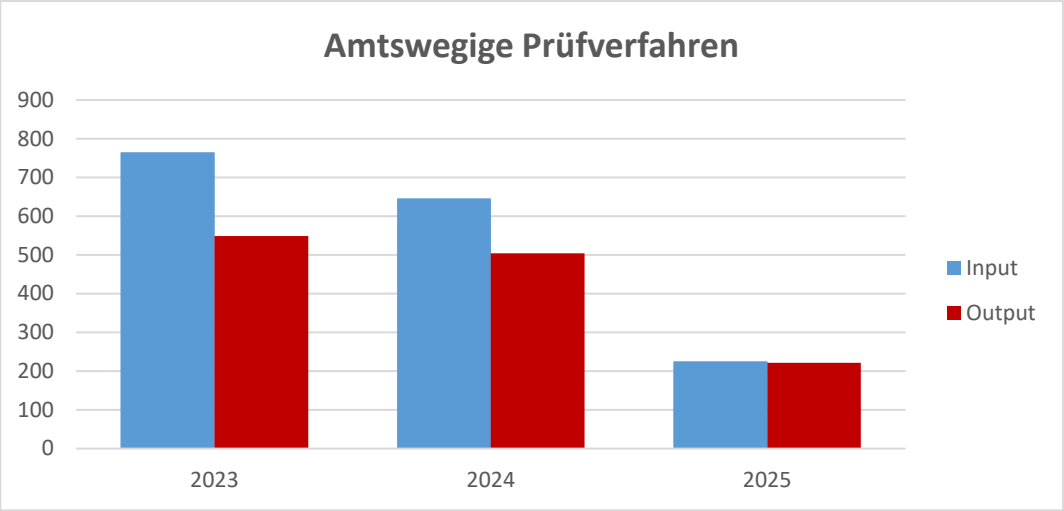
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2023	2024	**2025**	2023	2024	**2025**
Sicherheitsverletzungen grenzüberschreitend (im Ausland einlangend)	26	9	**20**	13	3	**12**
VERFAHREN VOR DEM BUNDESVERWALTUNGSGERICHT						
Verfahren vor dem BVwG - gesamt	613	301	**453**			
davon Bescheidbeschwerden	579	245	**345**			
davon Säumnisbeschwerden	34	56	**108**			
VERFAHREN VOR DEM VERWALTUNGSGERICHTSHOF						
Verfahren vor dem VwGH - gesamt			**126**			

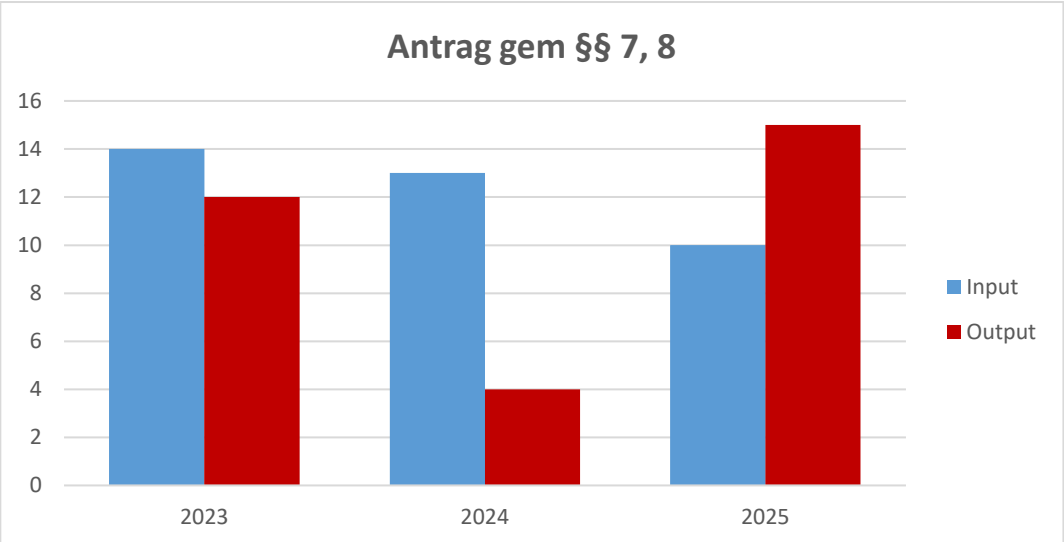
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2023	2024	**2025**	2023	2024	**2025**
VERFAHREN VOR DEM VERFASSUNGSGERICHTSHOF						
Verfahren vor dem VfGH - gesamt			**7**			
RECHTSAUSKÜNFTE/ANFRAGEN						
Schriftliche Rechtsauskünfte	1842	1935	**2498**	1842	1935	**2498**
Telefonische Rechtsauskünfte		224	**293**		224	**293**
Telefonische Anfragen, welche im Rahmen der Kanzleitätigkeit erledigt wurden		ca. 5.500	**ca. 6700**		ca. 5.500	**ca. 6700**
Schriftverkehr mit Behörden	185	265	**256**	185	265	**256**
Schriftverkehr mit privaten Einrichtungen		105	**139**		105	**139**
Allgemeine Anfragen aus dem Ausland	68	56	**67**			
Amtshilfeersuchen international über IMI einlangend (Art. 61 DSGVO)	624	612	**631**			
Amtshilfeersuchen international ausgehend (Art. 61 DSGVO)	242	199	**94**			
SONSTIGES						
Anträge auf Genehmigung nach §§ 7 und 8 DSG (wissenschaftliche Forschung u. Statistik)	14	13	**10**	12	4	**15**

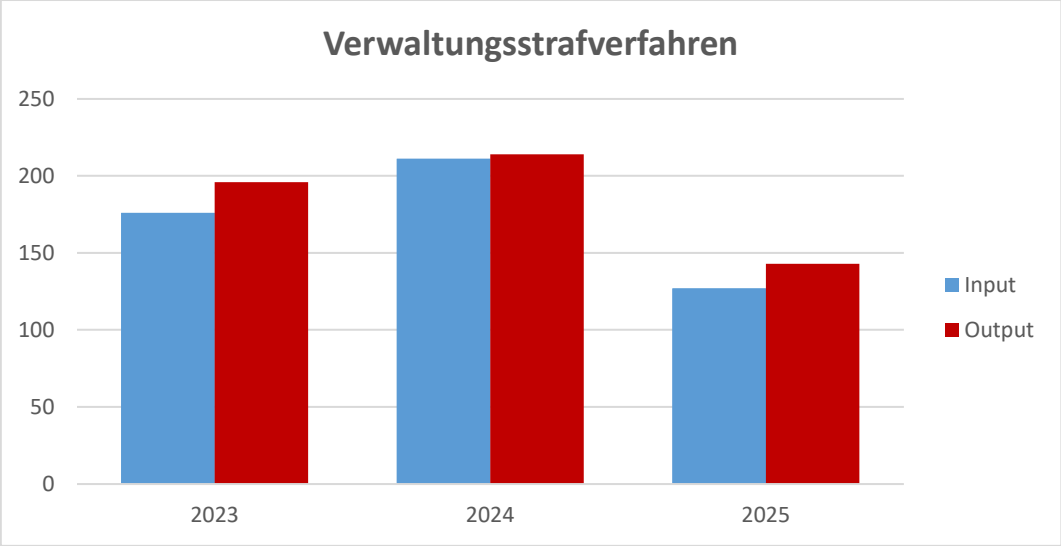
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2023	2024	**2025**	2023	2024	**2025**
Konsultationsverfahren	1	1	0	2	2	**0**
Anträge auf Genehmigung im internationalen Datenverkehr	0	0	**0**	0	0	**0**
Anträge auf Genehmigung von Verhaltensregeln	0	1	**1**	0	1	**0**
Co-Reviews (Art. 64 Abs. 1 DSGVO)		4	**2**		4	**2**
Genehmigung BCR (International)	0	0	**1**	0	0	**1**
Zertifizierungskriterien (Art. 42 DSGVO)	2	1	**0**	1	2	**1**
Akkreditierte Zertifizierungsstellen		1	**0**		1	**1**
Meldungen von Datenschutzbeauftragten	642	610	**618**	642	610	**618**

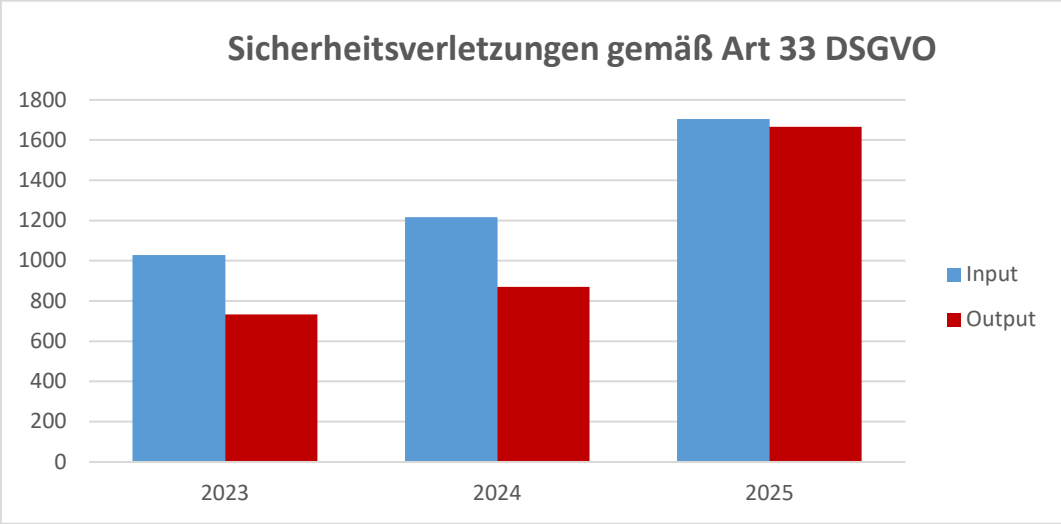
Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2023	2024	**2025**	2023	2024	**2025**
Auskunft und Löschung aus dem Schengen Information System (SIS)	336	285	**2293**	336	285	**2293**
Geltendmachung von Betroffenenrechten gegenüber der DSB		50	**152**		50	**152**
Auskunftsbegehren nach dem Informationsfreiheitsgesetz (IFG)			**29**			**29**

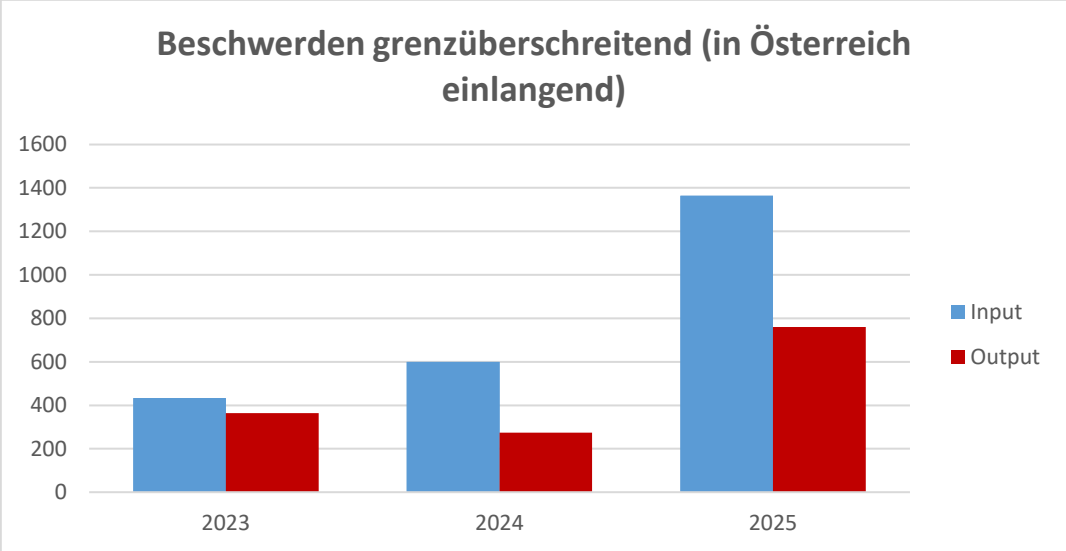

Individualbeschwerden
6000
5000
4000
3000
2000
1000
0
2023
2024
2025
Input
Output

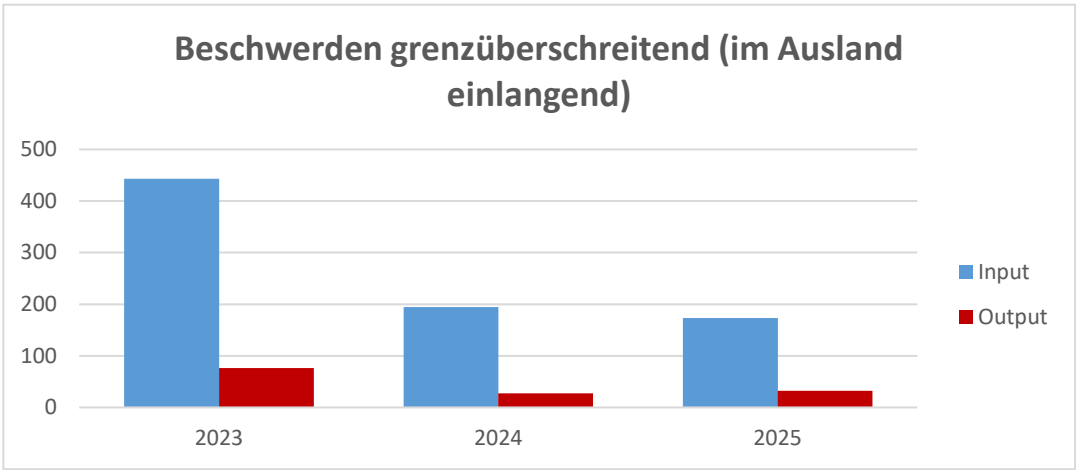

Amtswegige Prüfverfahren
900
800
700
600
500
400
300
200
100
0
2023
2024
2025
Input
Output

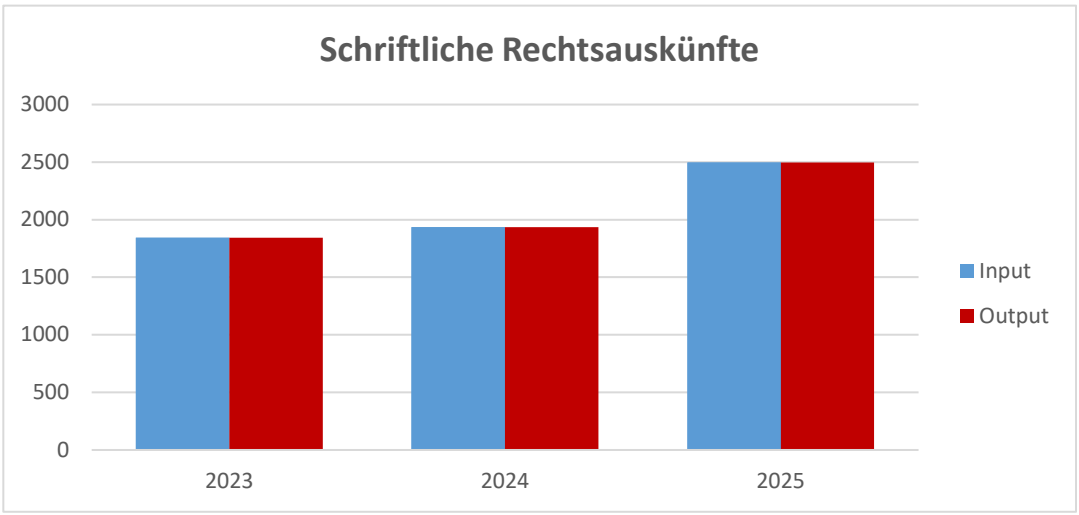

Antrag gem §§ 7, 8
16
14
12
10
8
6
4
2
0
2023
2024
2025
Input
Output


Verwaltungsstrafverfahren
250
200
150
100
50
0
2023
2024
2025
Input
Output


Sicherheitsverletzungen gemäß Art 33 DSGVO
1800
1600
1400
1200
1000
800
600
400
200
0
2023
2024
2025
Input
Output


Beschwerden grenzüberschreitend (in Österreich einlangend)
1600
1400
1200
1000
800
600
400
200
0
2023
2024
2025
Input
Output


Beschwerden grenzüberschreitend (im Ausland einlangend)
500
400
300
200
100
0
2023
2024
2025
Input
Output


Schriftliche Rechtsauskünfte
3000
2500
2000
1500
1000
500
0
2023
2024
2025
Input
Output

4.2 Erstsichtung von Anzeigen bzw. Anregungen an die DSB

Die DSB hat im letzten Jahresbericht über die Einführung eines **„Erstsichtungssystems“**[9] berichtet. Dieses interne System stellt eine von mehreren Maßnahmen der DSB dar, um die Effizienz zu steigern.

Im Rahmen der Erstsichtung werden sämtliche externe Eingaben an die DSB, die keine Beschwerden im Sinne des Art. 77 DSGVO sind, sondern eine Anregung, dass die DSB einen angezeigten Sachverhalt näher prüfen und bestimmte Abhilfemaßnahmen ergreifen soll, durch Mitarbeiter:innen der Abteilung V. geprüft.

Diese Anzeigen an die DSB werden nach Eingaben gefiltert, die **substantiiert** sind, einen für die DSB **relevanten Verstoß** darlegen und einen konkreten Anfangsverdacht für die Einleitung eines Ermittlungsverfahrens liefern. Auch sonstige Eingaben an die DSB, die aufgrund des Inhalts keinem konkreten Verfahren der DSB zugeordnet werden können, werden dieser Erstsichtung unterzogen.

Ziel der Erstsichtung ist es, die für die DSB relevanten Eingaben **rasch zu sichten und dem richtigen Verfahren zuzuführen**, sofern die Einleitung eines Verfahrens erforderlich erscheint.

Wenn ein Anfangsverdacht besteht, wird zudem im Zuge der Erstsichtung der Eingaben geprüft, ob das Auslangen mit einem **Sensibilisierungsschreiben** der DSB nach **Art. 57 Abs. 1 lit. d DSGVO** (ohne Ermittlungsverfahren) gefunden werden kann. Diese Erledigung stellt eine schriftliche Information der DSB in Bezug auf die einschlägige Rechtslage dar. Verantwortliche und Auftragsverarbeiter werden mit einem solchen Schreiben auf einen vermeintlichen Verstoß sowie die geltende Rechtslage hingewiesen (**Art. 58 Abs. 1 lit. d DSGVO**).

Im Berichtszeitraum 2025 wurden insgesamt **1800 Eingaben der Erstsichtung zugeführt:**

- Alle Eingaben konnten bis Ende des Jahres gesichtet und abschließend in der Erstsichtung behandelt werden.
- 1020 Eingaben wurden nach der Erstsichtung ohne weitere Maßnahmen abgelegt (Einstellung).
- Bei 335 Eingaben konnte das Auslangen mit einem Sensibilisierungsschreibens gefunden werden.
- Bei 443 Eingaben wurde ein Verfahren eingeleitet bzw. eine Prüfung von Maßnahmen vorgenommen.
- Von den rund 1800 Eingaben betraf der überwiegende Großteil (konkret 666 Eingaben) einen Sachverhalt mit einer Videoaufnahme (z.B. stationäre Videokameras oder Dash-Cam-Anlagen). Davon wurden 254 Fälle mit einer Sensibilisierung erledigt und 289 Eingaben wurden in der Erstsichtung eingestellt. Die restlichen Fälle sind einem Verfahren zugeführt worden.

9 siehe Datenschutzbericht 2024 unter Punkt 3.1.2 *„Maßnahmen zur Effiziensteigerung“.*

4.3 Verfahren und Auskünfte

4.3.1 Individualbeschwerden

Die DSB veröffentlicht seit 1. September 2025 vermehrt (auch nicht rechtsrechtskräftige) Entscheidungen im RIS, weshalb in Folge nur mehr jene Entscheidungen näher beleuchtet werden, die aufgrund ihres Inhalts und ihrer Tragweite besonders wichtig erscheinen.

1. Bescheid vom 4. Februar 2025, OZ: 2025-0.021.375 (GZ: D124.1328/24)
Videoüberwachung bei Pflegetätigkeiten

Eine Pflegerin beschwerte sich im vorliegenden Fall aufgrund von Videokameras, die sie bei der Verrichtung ihrer Pflegetätigkeit in der Wohnung einer pflegebedürftigen Person aufzeichneten. Dadurch sah sie sich im Recht auf Geheimhaltung verletzt. Der Erwachsenenvertreter der zu pflegenden Person hatte die Kameras nach einem Sturz ebendieser installiert. Die Kameras sollten sicherstellen, dass bei Notfällen schnellstmöglich jemand vor Ort sein könne.

Die DSB gab der vorliegenden Beschwerde statt und ordnete an, die Nutzung der Kameras derart einzuschränken, das während der Pflegetätigkeit keine Aufnahmen angefertigt werden. Eine Videoüberwachung während der Anwesenheit von Pflegepersonal erschient jedenfalls nicht erforderlich. Der Gesundheitszustand und das allgemeine Wohlbefinden der pflegebedürftigen Person wird bei Anwesenheit des Pflegepersonals von diesem kontrolliert.

Der Bescheid ist rechtskräftig.

2. Bescheid vom 24. Februar 2025, OZ: 2025-0.045.624 (GZ: D124.1905/24)
Veröffentlichung personenbezogener Daten im Rahmen von Bürgerjournalismus

Die DSB hat sich in dieser Entscheidung erstmals mit Datenverarbeitungen im Rahmen von Bürgerjournalismus gemäß § 9 Abs. 1a DSG idF BGBl. I Nr. 62/2024 (sog. „Medienprivileg“), befasst. Diese Regelung betrifft journalistische Tätigkeiten von Privatpersonen („Bürgerjournalismus“), etwa wie im gegenständlichen Fall auf einer Diskussionsplattform.

Vorliegend beschwerte sich eine Führungskraft einer regierungsnahen Organisation über die Veröffentlichung eines von ihr verfassten Schreibens auf einer Diskussionsplattform. Das Schreiben enthielt dabei die dienstlichen Kontaktdaten der beschwerdeführenden Führungskraft. Durch die Veröffentlichung erblickte diese eine Verletzung im Recht auf Geheimhaltung.

Die DSB kam zu dem Ergebnis, dass die Veröffentlichung des Schreibens im gegebenen Fall zulässig war. Der Veröffentlichung lagen journalistische Zwecke zugrunde, und erblickte die DSB darin ein berechtigtes Interesse, dass der Öffentlichkeit diese Information zur Kenntnis gebracht werden. Die Veröffentlichung war zudem erforderlich und verhältnismäßig.

Der Bescheid ist rechtskräftig.

3. Bescheid vom 29. Juli 2025, OZ: 2024-0.368.729 (GZ: D124.0840/24)
Veröffentlichung von Angaben zu Lebensmittelabfällen und -spenden auf einer staatlichen Onlineplattform (EDM-Portal)

Im vorliegenden Fall erhob ein Einzelunternehmer Beschwerde wegen Veröffentlichung von personenbezogenen Daten, konkret Name, Anzahl der Verkaufsstellen und Angaben zu Lebensmittelabfällen und -spenden. Dadurch sah sich dieser im Recht auf Geheimhaltung verletzt.

Die DSB hielt zunächst fest, dass es sich bei den veröffentlichten Informationen um personenbezogene Daten handelt, da diese direkt einer identifizierbaren natürlichen Person zugeordnet werden können. Die DSB erachtete die Veröffentlichung als gerechtfertigt. Die Veröffentlichung erfolgte auf Grundlage von gesetzlichen Bestimmungen, vorrangig des Abfallwirtschaftsgesetzes. Aus Sicht der DSB besteht ein öffentliches Interesse an Informationen zu Umweltschutz sowie an Information von Spendenmengen im Vergleich zu Abfallmengen und letztendlich an Reduktion der Lebensmittelverschwendung. Zweck des EDM-Portals ist dabei, Transparenz über Lebensmittelabfälle und -spenden zu schaffen. Die Beschwerde wurde im Ergebnis abgewiesen.

Der Bescheid ist nicht rechtskräftig.

4. Bescheid vom 8. Oktober 2025, OZ: 2025-0.477.534 (GZ: D135.027)
Nutzung von „Microsoft 365 Education" in Bildungseinrichtungen
In diesem Verfahren befasste sich die DSB mit einer Beschwerde einer schulpflichtigen Person, vertreten durch einen Obsorgeberechtigten, gegen die Schulleitung ihrer Bildungseinrichtung, die zuständige Bildungsdirektion, das Bildungsministerium sowie Microsoft mit Sitz in den USA. Im Kern wurde eine Verletzung im Recht auf Information und im Recht auf Auskunft in Bezug auf die Bereitstellung und Nutzung von Microsoft 365 Education in der betroffenen Bildungseinrichtung geltend gemacht.

Die DSB hat nach einem umfangreichen Ermittlungsverfahren zunächst in Bezug auf die datenschutzrechtliche Rollenverteilung festgehalten, dass die Schulleitung der Bildungseinrichtung und das Bildungsministerium als gemeinsam Verantwortliche anzusehen sind, da sie die wesentlichen Entscheidungen für den Einsatz von Microsoft 365 Education getroffen haben. Die zuständigen Bildungsdirektion wurde von der DSB mangels faktischer Einflussnahme auf die Entscheidungsprozesse nicht als Verantwortliche qualifiziert. Des Weiteren wurde auch Microsoft als Verantwortliche für jene Verarbeitungstätigkeiten angesehen, die sie im Rahmen der Bereitstellung von Microsoft 365 Education zu ihren eigenen Zwecken verarbeitet.

Ferner stellte die DSB eine Verletzung im Recht auf Information und im Recht auf Auskunft fest und trug der Schulleitung und dem Bildungsministerium u.a. auf, der betroffenen Person Informationen und Auskunft zu den bei der Nutzung von Microsoft 365 Education anfallenden, sie betreffenden, Inhaltsdaten, Verbindungsdaten, und Cookie-Daten sowie Datenübermittlungen in Drittländer zu erteilen. Microsoft wurde von der DSB aufgetragen, der betroffenen Person alle personenbezogenen Daten, die Microsoft für eigene Zwecke verarbeitet, zu beauskunften und die Zwecke verständlich zu beschreiben.

Der Bescheid ist nicht rechtskräftig, jedoch mit entsprechendem Vermerk im RIS abrufbar.[10]

5. Bescheid vom 14. Oktober 2025, OZ: 2025-0.328.963 (GZ: D124.2695/24)
Erteilung einer Auskunft über das Bestehen einer automatisierten Entscheidungsfindung sowie aussagekräftige und verständliche Information über die darin involvierte Logik und die Tragweite und die angestrebten Auswirkungen der Verarbeitung
Im vorliegenden Verfahren hatte sich die DSB mit einer Beschwerde aufgrund einer behaupteter-maßen unvollständig erteilten Auskunft zu befassen. Die beschwerdeführende Partei hatte zuvor einen Antrag auf Auskunft an eine Kreditauskunftei gestellt um herauszufinden, auf welchen

10 Siehe https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=cc42849a-efda-4a81-b146-7406e3ca74fa&Position=1&SkipToDocumentPage=True&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=30.01.2026&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20251008_2025_0_477_534_00.

Grundlagen bestimmte Bonitäts-Scores berechnet wurden. Die Auskunft habe zwar grundlegende Daten enthalten, aber keine transparenten, verständlichen Angaben zur Berechnungslogik, Herkunft der Daten oder Empfängern der Daten.

Die DSB gab der Beschwerde statt und hielt fest, dass die zur Verfügung gestellten Informationen nicht vollständig, verständlich und transparent waren. Es fehlten Erklärungen zur Logik und Berechnung der automatisierten Score-Werte, zur Herkunft der Daten sowie zu den Empfänger der Daten.

Die DSB trug der beschwerdegegnerischen Partei mitunter auf, eine vollständige und verständliche Auskunft zu erteilen und zu erläutern, anhand welcher konkreten personenbezogenen Daten und nach welchen mathematisch-statistischen Prinzipien der Scoring Wert berechnet wird, transparent die Bedeutung der einzelnen Eingabedaten für die Berechnung des Ergebnisses zu erläutern und die möglichen Auswirkungen des Scoring-Wertes auf potenzielle Vertragsabschlüsse zu beschreiben.

Der Bescheid ist nicht rechtskräftig.

4.3.2 Grenzüberschreitende Fälle der DSB

Die DSB befasst sich neben nationalen Verfahren auch mit Fällen, die einen grenzüberschreitenden Sachverhalt aufweisen, z.B. wenn eine **Verfahrenspartei nicht in Österreich ansässig** ist. Dies betrifft von Betroffenen erhobene Beschwerden, amtswegige Prüfverfahren, Mitteilungen über Sicherheitsverletzungen gemäß Art. 33 DSGVO sowie Genehmigungsverfahren.

Bei grenzüberschreitenden Fällen ist danach zu unterschieden, ob die DSB das Verfahren in Alleinzuständigkeit führt und am Ende selbst eine materielle Entscheidung erlässt, oder ob eine Zuständigkeit weiterer Aufsichtsbehörden gegeben ist, die dann in das Verfahren einzubinden sind.

Hat eine:ein Verantwortliche:r oder ein:eine Auftragsverarbeiter:in keine Niederlassung bzw. keinen Sitz in einem anderen Mitgliedstaat der Europäischen Union bzw. des Europäischen Wirtschaftsraumes[11], kann eine Zuständigkeit der DSB gegeben sein, wenn der **räumliche Anwendungsbereich der DSGVO aufgrund des sog. Marktortprinzips**[12] eröffnet ist. In diesem Zusammenhang ist die DSB etwa regelmäßig mit einer beträchtlichen Anzahl an Beschwerden befasst, die gegen in Drittländern ansässige Anbieter von Online-Glückspielen erhoben werden.

Wird hingegen bei der DSB eine Beschwerde eingebracht, die sich sich gegen eine:einen Verantwortliche:n oder Auftragsverarbeiter:in, der:die in einem anderen Mitgliedstaat der Europäischen Union bzw. des Europäischen Wirtschaftsraums niedergelassen ist, richtet, liegt in der Regel eine „grenzüberschreitende Datenverarbeitung“ iSd. **Art. 4 Z 23 DSGVO** vor. In weiterer Folge ist ein sog. **„One-Stop-Shop“** Verfahren gemäß **Art. 56 DSGVO iVm. Art. 60 DSGVO** zu führen.[13] In einem solchen Verfahren sind im ersten Schritt die federführende Aufsichtsbehörde sowie die betroffenen Aufsichtsbehörden zu bestimmen. 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 oder einziger Niederlassung in Österreich richtet.

---

11 EU-Mitgliedstaaten sowie Norwegen, Island und Liechtenstein.

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

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.

Im Hinblick auf die Führung von „One-Stop-Shop“ Verfahren hat der Unionsgesetzgeber im Berichtszeitraum eine **Verordnung** erlassen, **mit welcher zusätzliche Verfahrensregeln für die Durchsetzung der DSGVO** festgelegt werden.[14] Diese Verordnung tritt am 2. April 2027 in Geltung und legt u.a. Fristen für bestimmte Verfahrenshandlungen bzw. -abschnitte sowie zum Teil auch neue Verfahrensschritte fest, was einer entsprechenden Vorbereitung der DSB auf den neuen Rechtsrahmen bedarf.

Bei Uneinigkeiten zwischen Aufsichtsbehörden im Rahmen grenzüberschreitender Verfahren sieht **Art. 65 DSGVO** ein **Streitbeilegungsverfahren vor dem EDSA** vor, welcher mit verbindlichem Beschluss über den Streitfall entscheiden kann. Ferner kann unter außergewöhnlichen Umständen auf begründeten Antrag einer Aufsichtsbehörde ein **Dringlichkeitsverfahren** vor dem EDSA eingeleitet werden. Im Jahr 2025 hat der EDSA keine verbindlichen Beschlüsse nach **Art. 65 Abs. 1** oder nach Art. 66 Abs. 2 und 3 DSGVO erlassen.

Bei der DSB wurden im Berichtsjahr 2025 insgesamt **1364 grenzüberschreitende Beschwerden** eingebracht. In **1038 Fällen** richteten sich die Beschwerden gegen Verantwortliche mit Sitz in einem anderen Mitgliedstaat der EU bzw. im EWR und es wurde in diesen Fällen ein One-Stop-Shop Verfahren eröffnet. In **326 Fällen** wurden bei der DSB Beschwerden gegen Verantwortliche oder Auftragsverarbeiter:innen, welche in einem Drittland niedergelassen sind, anhängig gemacht und die DSB hat in **173 Fällen** mit Drittlandsbezug eine verfahrensbeendende Erledigung erlassen, wobei hier Beschwerdeverfahren gegen in Drittländern ansässige Anbieter von Online-Glückspielen einen wesentlichen Teil ausmachten.

Umgekehrt sind bei der DSB im Berichtsjahr 2025 insgesamt **1207 grenzüberschreitende Beschwerden**, welche bei einer anderen Aufsichtsbehörde im EWR eingebracht wurden, eingelangt und die DSB hat sich in **152 Fällen** als betroffene Aufsichtsbehörde und in **21 Fällen** als **federführende Aufsichtsbehörde gem. Art. 56 DSGVO** deklariert.

Im Rahmen der grenzüberschreitenden Zusammenarbeit innerhalb und außerhalb eines konkreten Verfahrens machte die DSB **209 Mal** von der **gegenseitigen Amtshilfe iSd. Art. 61 DSGVO** Gebrauch und wurde selbst in **631 Fällen** von anderen Aufsichtsbehörden kontaktiert.

Ausgewählte Entscheidungen der DSB im Jahr 2025 werden in **Kapitel 4.3.1.1.** vorgestellt.

4.3.3 Rechtsauskünfte an Bürger:innen

Die DSB stellt auf ihrer **Webseite** (abrufbar unter: https://dsb.gv.at/faq/faqs, https://dsb.gv.at/informationsfreiheitsgesetz/datenschutz-und-informationsfreiheit-fragen-und-antworten- und unter https://dsb.gv.at/kuenstlichebrintelligenz/kuenstliche-intelligenz-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 Datenschutzbehörde“** (abrufbar unter: www.dsb.gv.at) einen raschen Überblick über die neuesten Entwicklungen im Datenschutzrecht.

---

14 Verordnung (EU) 2025/2518 des Europäischen Parlaments und des Rates vom 26. November 2025 zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679, ABl. L, 2025/2518, 12.12.2025.

Darüber hinaus **beantwortet die DSB allgemeine Anfragen** zum geltenden Datenschutzrecht sowohl **schriftlich**, als auch zu eingeschränkten Zeiten **telefonisch**.

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).

4.3.4 Genehmigungen im internationalen Datenverkehr

Die DSGVO sieht eine **weitgehende Genehmigungsfreiheit** für den internationalen Datenverkehr mit 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 Aufsichtsbehörde 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 Aufsichtsbehörde unter Anwendung des Kohärenzverfahrens gemäß **Art. 63 ff DSGVO** genehmigt werden.[18] Hierbei ist eine enge Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden 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 abgewogen werden, ob die Zulässigkeit der Datenübermittlung nicht einfacher und effizienter durch andere geeignete Garantien im Sinne

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, abrufbar in englischer Sprache unter https://www.edpb.europa.eu/system/files/2023-06/edpb_recommendations_20221_bcr-c_v2_en.pdf, sowie den Recommendations 1/2026 on the Application for Approval and on the elements and principles to be found in Processor Binding Corporate Rules, abrufbar in englischer Sprache unter https://www.edpb.europa.eu/system/files/2026-01/edpb_recommendations202601_bcr-p_v1_en.pdf (derzeit in öffentlicher Begutachtung) des Europäischen Datenschutzausschusses zu entnehmen.

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.

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 gemäß Art. 40 DSGVO** und **Zertifizierungen** gemäß **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 wurde im Jahr 2025 **ein** Genehmigungsantrag betreffend **verbindliche interne Datenschutzvorschriften nach Art. 46 Abs. 2 lit. b iVm. Art. 47 DSGVO** gestellt, welcher in weiterer Folge zurückgezogen wurde. Ferner hat sich die DSB im Berichtszeitraum in **zwei** Fällen als „Co-Reviewer" von genehmigungspflichtigen Garantien iSv. Kapitel V DSGVO, die bei einer anderen Aufsichtsbehörde zur Genehmigung vorgelegt wurden, beteiligt.

4.3.5 Genehmigungen nach §§ 7 und 8 DSG

§ 7 DSG regelt die Voraussetzungen für die Verarbeitung 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.

Gemäß **§ 7 Abs. 3** sowie **§ 8 Abs. 3 DSG** kann es unter bestimmten Umständen erforderlich sein, vor dieser Verarbeitung personenbezogener Daten eine **Genehmigung der DSB** einzuholen. Hierbei ist zu beachten, dass in einem solchen Genehmigungsverfahren grundsätzlich **Gebühren** anfallen.

Im Rahmen der **§§ 7 und 8 DSG** langten bei der DSB im Jahr 2025 insgesamt **34 Anträge** ein.

Hinsichtlich **§ 7 Abs. 3 DSG** ist die Entscheidung der DSB vom 28. Juli 2025 zu **OZ: 2025-0.587.665 (GZ: D202.354)** hervorzuheben. Mit dieser Entscheidung hat die DSB den Antrag genehmigt, personenbezogene Daten durch Aufzeichnungen von Bild- und Videodaten von Personen, die das Ars

---

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.

Electronica Festival 2025 besuchen, auf dem Festivalgelände und für die Dauer des Festivals zu ermitteln und für wissenschaftliche Forschungszwecke auszuwerten. Das Hauptziel dieses Projekts war es, die Öffentlichkeit für die allgegenwärtige Gesichtserkennungstechnologie und deren Auswirkungen auf die Privatsphäre zu sensibilisieren. Die Antragstellerin wurde angewiesen, die stationären oder drohnengetragenen Messapparaturen, welche Aufzeichnungen des öffentlichen Raums vornehmen, mit einem Schild oder Aufkleber zu kennzeichnen. Auf dem Schild musste die Datenerfassung kenntlich gemacht werden, zudem mussten der Name der Antragstellerin und ein Verweis auf weiterführende Informationen gemäß Art. 13 DSGVO (etwa auf der Webseite der Antragstellerin) ersichtlich sein. Der Zugang zu den Aufzeichnungen mit personenbezogenen Daten war durch die Antragstellerin in geeigneter Weise gemäß Art. 32 Abs. 1 DSGVO abzusichern. Die Einsicht in die und die Auswertung der aufgezeichneten personenbezogenen Daten durfte nur durch bestimmte, geschulte und gemäß § 6 DSG aufgeklärte Mitarbeiter:innen bzw. deren Auftragsverarbeiter:innen erfolgen. Nach Abschluss des Forschungsprojekts waren die Daten zu löschen. Eine Veröffentlichung personenbezogener Daten durfte nur in anonymisierter Form erfolgen.

Mit Bescheid vom 29. Jänner 2025 über die Erteilung einer Genehmigung gemäß **§ 8 Abs. 3 DSG** zu **OZ: 2025-0.038.404 (GZ: D202.342)** wies die DSB den Antrag der Antragstellerin zurück. Die Antragstellerin ersuchte die DSB um Genehmigung der Übermittlung von Adressdaten von bei ihr versicherten Personen über 65 Jahre für ein österreichweites Forschungsprojekt einer Medizinischen Universität. An dieser Studie sollten möglichst viele Personen in Österreich teilnehmen, die über 65 Jahre alt sind. Aufgrund der immens hohen Anzahl von etwa 1,35 Millionen Betroffenen würde die Einholung von Einwilligungen einen unverhältnismäßig hohen Aufwand erfordern. Entgegen dem Vorbringen der Antragstellerin lagen die Voraussetzungen gemäß § 8 Abs. 2 Z 2 lit. a DSG jedoch aus nachfolgenden Gründen vor: Eine Ausnahme vom Erfordernis der Einwilligung der betroffenen Personen liegt nämlich vor, wenn eine Beeinträchtigung der Geheimhaltungsinteressen der betroffenen Personen angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung unwahrscheinlich ist und bei einer beabsichtigten Übermittlung der Adressdaten an Dritte ein öffentliches Interesse an der Benachrichtigung oder Befragung besteht. Die Kriterien, anhand derer die Adressdaten selektiert werden, müssen demnach solche sein, welche die Geheimhaltungsinteressen der betroffenen Personen voraussichtlich nicht beeinträchtigen. Da im vorliegenden Fall ausschließlich nach dem Alter selektiert wird, war nicht von einer Beeinträchtigung der Geheimhaltungsinteressen der betroffenen Personen auszugehen. Ein öffentliches Interesse war ebenfalls zu bejahen, schließlich handelte es sich um die größte in Österreich durchgeführte digitale Studie, deren Hauptziel darin besteht, eine digitale Screening- und Interventionsstrategie zu entwickeln und in einer breit angelegten, digitalen und randomisierten Studie zu testen, ob sich dadurch Schlaganfälle reduzieren lassen. Da somit alle Voraussetzungen des § 8 Abs. 2 Z 2 lit. a DSG vorgelegen haben, war gemäß § 8 Abs. 3 DSG auch keine Genehmigung der DSB notwendig. Der Antrag war daher spruchgemäß zurückzuweisen.

4.3.6 Amtswegige Prüfverfahren

Die DSB leitete im Jahr 2025 225 **amtswegige Prüfverfahren** ein. Im Berichtszeitraum wurden **222 amtswegige Prüfverfahren enderledigt**.

Ausgewählte Entscheidungen:

1. Bescheid vom 19. Mai 2025; OZ: 2025-0.327.266 (GZ: D213.3166)
Umfassende Videoüberwachung in Kassenräumlichkeiten, Beschränkung der Verarbeitung gemäß Art. 58 Abs. 2 lit. f DSGVO
Aufgrund einer anonymen Anzeige leitete die DSB ein amtswegiges Prüfverfahren gegen eine

öffentliche Stelle wegen des Einsatzes von Videoüberwachung in Kassenräumlichkeiten ein. Gegenstand des Verfahrens war eine umfangreiche Videoüberwachungsanlage, die sowohl Kundenbereiche als auch interne Arbeits- und Kassenbereiche erfasste. Die Videoüberwachung wurde mit dem Schutz von Eigentum, Bargeldbeständen sowie der Sicherheit der Mitarbeitenden begründet.

Die DSB stellte fest, dass die Videoüberwachung eine Verarbeitung personenbezogener Daten darstellt und die betroffene Organisationseinheit als datenschutzrechtlich Verantwortliche anzusehen ist. Die Datenverarbeitung wurde der Privatwirtschaftsverwaltung zugeordnet, sodass Art. 6 Abs. 1 lit. f DSGVO grundsätzlich als Rechtsgrundlage herangezogen werden konnte. Ein berechtigtes Interesse am Schutz von Eigentum und Mitarbeitenden wurde aufgrund einer konkreten Gefährdungslage bejaht.

Die Videoüberwachung in öffentlich zugänglichen Kassen- und Wartebereichen wurde als geeignet, erforderlich und verhältnismäßig beurteilt, da sie räumlich und zeitlich begrenzt sowie transparent ausgestaltet war. Demgegenüber erwies sich die umfassende Überwachung interner Arbeitsplätze als unverhältnismäßig, weil sie intensiv in die Rechte der Beschäftigten eingriff und gelindere Mittel zur Verfügung gestanden wären. Insoweit überwogen die Interessen der Betroffenen, weshalb diese Verarbeitung als rechtswidrig qualifiziert wurde. Die DSB ordnete daher die Anpassung der betreffenden Kameras an, um einen rechtskonformen Zustand herzustellen.

Der Bescheid ist rechtskräftig.

2. Bescheid vom 11. Februar 2025; OZ: 2024-0.195.679 (GZ: D213.2544)
Zur Unzulässigkeit von Straßenfotografie ohne Einwilligung trotz Berufung auf Kunstfreiheit, Anordnung gemäß Art. 58 Abs. 2 lit. g DSGVO
Die DSB führte aufgrund einer anonymen Anzeige ein amtswegiges Prüfverfahren gegen den Betreiber einer öffentlich zugänglichen Website durch, auf der er von ihm angefertigte Straßenfotografien veröffentlicht. Auf der Website befanden sich Fotos von identifizierbaren Personen, darunter Kinder, Personen beim Essen, Frauen mit exponierter Darstellung des Brustbereichs sowie Personen, aus deren Erscheinungsbild religiöse Überzeugungen ableitbar waren.

Der Verantwortliche holte für diese Bildaufnahmen und deren Veröffentlichung weder durchgehend Einwilligungen ein noch informierte er die Betroffenen systematisch gemäß Art. 13 DSGVO.

Die Anfertigung und Veröffentlichung der Fotos stellen eine Verarbeitung personenbezogener Daten im Sinne der DSGVO dar. Zwar kann sich der Verantwortliche grundsätzlich auf die Kunstfreiheit gemäß Art. 13 EU-GRC iVm Art. 85 DSGVO und § 9 Abs. 2 DSG berufen, jedoch bleiben die Grundsätze des Art. 5 DSGVO, insbesondere Rechtmäßigkeit, Transparenz und Datenminimierung, anwendbar.

Im Rahmen der erforderlichen Interessenabwägung überwogen bei einigen der abgebildeten Personen die Interessen der betroffenen Personen, da Kinder als besonders schutzwürdig gelten und die Fotos teilweise sensible Daten nach Art. 9 DSGVO wie religiöse Überzeugungen offenlegten. Zudem stellten die exponierte Darstellung weiblicher Körperteile sowie Aufnahmen von Personen in privaten Alltagssituationen (Essen), wo sie nicht mit Fotoaufnahmen rechnen müssen, erhebliche Eingriffe in das Persönlichkeitsrecht dar.

Mangels wirksamer Einwilligung oder sonstiger tragfähiger Rechtsgrundlage war bereits die Herstellung der Fotos unzulässig, weshalb auch deren Veröffentlichung rechtswidrig war. Der Leistungsauftrag zur Löschung gemäß Art. 58 Abs. 2 lit. g DSGVO erwies sich daher als angemessen.

Der Bescheid ist rechtskräftig.

4.3.6.1 Schwerpunktprüfung 2025

Im Jahr 2025 führte die DSB **amtswegige Schwerpunktprüfungen** bei allen **Landespolizeidirektionen** durch. Gegenstand dieser Prüfungen war die Einhaltung der Vorgaben der DSGVO sowie des **3. Hauptstücks des DSG**, in welchem die Richtlinie (EU) 2016/680 umgesetzt wurde.

Im Fokus der Prüfverfahren standen insbesondere die Einhaltung der gesetzlich vorgeschriebenen **Dokumentationspflichten sowie die spezifischen datenschutzrechtlichen Anforderungen**, die für die Verarbeitung personenbezogener Daten im polizeilichen Bereich gelten. Zusätzlich wurden im Rahmen des **Coordinated Enforcement Framework (CEF)**[25] des EDSA das Recht auf Löschung und die damit im Zusammenhang stehenden Speicherfristen überprüft.

Die Prüfverfahren wurden nunmehr abgeschlossen. Aus Sicht der DSB ergaben sich dabei **keine Beanstandungen**. Damit bestätigt sich, dass die Verantwortlichen im polizeilichen Bereich den Datenschutz ernst nehmen und in der Praxis wirksam umsetzen.

Die DSB wird auch im Jahr 2026 amtswegige Schwerpunktprüfungen durchführen.[26]

4.3.7 Beschwerdeverfahren vor dem BVwG, einschließlich Säumnisbeschwerden

4.3.7.1 Beschwerdeverfahren in Administrativsachen

1. Erkenntnis des BVwG vom 24. Februar 2025, W298 2296144-1
Zulässigkeit der Speicherung von Bonitätsdaten durch Kreditauskunfteien

Dem Erkenntnis des BVwG vorangegangen war eine Beschwerde an die DSB wegen behaupteter Verletzung im Recht auf Löschung von negativen Zahlungserfahrungsdaten durch eine Kreditauskunftei. Die Kreditauskunftei verarbeitete Daten der beschwerdeführenden Partei zu vier bereits positiv erledigten Forderungen und lehnte die Löschung mit der Begründung ab, dass die Daten zu Zwecken der Bonitätsprüfung nach wie vor erforderlich seien.

Die DSB gab der Beschwerde nach erfolgter Interessensabwägung statt und sprach aus, dass die Zahlungserfahrungsdaten für die Beurteilung der Bonität nicht mehr relevant sind. Die DSB hielt fest, dass die Kreditauskunftei die Zahlungserfahrungsdaten über den Zeitpunkt der positiven Erledigung der Forderungen hinaus unrechtmäßig verarbeitet hat und trug die DSB demnach die Löschung auf. Dagegen erhob die Kreditauskunftei Bescheidbeschwerde.

Das BVwG führte mit Verweis auf die Rechtsprechung des EuGH zu C 26/22 und C 64/22 [SCHUFA Holding AG] zunächst aus, dass die Verarbeitung von Daten über Insolvenzen einen negativen Faktor bei der Beurteilung der Kreditwürdigkeit einer betroffenen Person darstellt und deren Verarbeitung den Interessen einer betroffenen Person beträchtlich schaden kann. Dies trifft ebenso auf Zahlungserfahrungsdaten zu, welche Kreditauskunfteien von Inkassounternehmungen

offengelegt wurden und die nicht aus öffentlichen Insolvenzregistern stammen. Für das wirtschaftliche Fortkommen einer betroffenen Person gestaltet es sich nicht weniger eingriffsintensiv, wenn Daten nicht gerichtlich betriebene Forderungen betreffen und eine bloße vorübergehende Schuldnersäumnis vorliegt.

---

25 https://www.edpb.europa.eu/news/news/2025 cef-2025-launch-coordinated-enforcement-right-erasure_de, abgerufen am 18.02.2026.
26 https://dsb.gv.at/aktuelles/information-zur-schwerpunktpruefung-2026, abgerufen am 18.02.2026.

Die Rechtsprechung des EuGH, wonach eine Speicherung von aus öffentlichen Registern stammenden Informationen über Insolvenzen natürlicher Personen durch private Wirtschaftsauskunfteien zum Zweck der Erteilung von Auskünften über die Kreditwürdigkeit einer Person für einen Zeitraum, der über die Speicherdauer der Daten in den öffentlichen Registern hinausgeht, nicht mit Art. 5 Abs. 1 lit. a iVm. Art. 6 Abs. 1 lit. f DSGVO im Einklang steht, ist nach Auffassung des BVwG verfahrensgegenständlich relevant. Unter Berücksichtigung der österreichischen Insolvenzordnung, dabei insbesondere § 256 Abs. 2 IO, sind Insolvenzdaten nach Abschluss des Insolvenzverfahrens in der Regel bis ein Jahr öffentlich abrufbar. Demnach sind Insolvenzdaten in der österreichischen Rechtsordnung mangels entgegenstehender individueller Gründe längstens ein Jahr nach schuldbefreiender Bezahlung zu löschen (vgl. Art. 5 Abs. 1 lit. a iVm. Art. 17 Abs. 1 lit. d DSGVO iVm. § 256 IO).

2. Beschluss des BVwG vom 24. April 2025, W298 2308675-1
Keine Verletzung der Unterrichtungspflicht durch die DSB
Mit vorliegendem Beschluss wies das BVwG eine Säumnisbeschwerde wegen Verletzung der Unterrichtungspflicht nach § 24 Abs. 7 DSG als unzulässig zurück.

Dem Beschluss vorangegangen war eine Beschwerde wegen behaupteter Verletzung im Recht auf Löschung. Die DSB hatte im Hinblick auf die Beschwerde ein Ermittlungsverfahren eingeleitet. Im Laufe des Ermittlungsverfahrens hat die beschwerdegegnerische Partei dem Löschbegehren der beschwerdeführenden Partei vollumfänglich entsprochen. Die DSB informierte demnach die beschwerdeführende Partei im Rahmen des Parteigehörs, dass sie die Beschwerde im Sinne des § 24 Abs. 6 DSG als erledigt erachtet. Der beschwerdeführenden Partei wurde freigestellt, begründet auszuführen, falls sie die ursprünglich behauptete Rechtsverletzung der nicht erfolgten Löschung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Weiters teilte die DSB mit, dass sie anderenfalls das Verfahren formlos einstellen wird. Eine Reaktion der beschwerdeführenden Partei auf dieses Schreiben erfolgte nicht, weshalb die DSB das Verfahren einstellte.

Die beschwerdeführende Partei erhob Beschwerde wegen Verletzung der Unterrichtungspflicht nach § 24 Abs. 7 DSG

Das BVwG hielt fest, dass keine Säumnis der DSB vorlag. Die DSB hatte die beschwerdeführende Partei über den Stand des Verfahrens und das Ergebnis der Ermittlung unterrichtet. Dadurch erblickte das BVwG keine Beschwer und kommt eine Feststellung einer Verletzung der Unterrichtungspflicht in der Vergangenheit nicht in Betracht.

3. Erkenntnis des BVwG vom 30. Juni 2025, W137 2253891-1
Finanzmarktaufsicht ist keine Empfängerin, wenn ihr personenbezogene Daten aufgrund ihrer gesetzlichen Untersuchungsbefugnissen zur Verfügung gestellt werden
Dem Erkenntnis des BVwG vorgelagert war eine Beschwerde an die DSB wegen behaupteter Verletzung im Recht auf Auskunft. Die Beschwerde war gegen ein Kreditinstitut gerichtet und bemängelte die dortige beschwerdeführende Partei im Wesentlichen die Vollständigkeit der erteilten Auskunft. Die beschwerdeführende Partei wollte insbesondere in Erfahrung zu bringen, ob ihre personenbezogenen Daten an unternehmensfremde Personen weitergegeben worden sind oder ob unternehmensfremde Personen in die Daten eingesehen haben oder darauf Zugriff genommen haben. Die Finanzmarktaufsicht hatte beim beschwerdegegnerischen Kreditinstitut eine Vor-Ort Prüfung nach § 30 Abs. 1 FM-GwG durchgeführt. Grund dieser war der Verdacht, dass Mittel der beschwerdeführenden Partei aus illegalen Quellen stammen.

Die DSB hatte vorliegend zu prüfen, ob die im Rahmen einer Finanzprüfung erfolgte Offenlegung von personenbezogenen Daten an die FMA von der beschwerdegegnerischen Partei nach Art. 15

Abs. 1 lit. c DSGVO zu beauskunften ist. Die DSB verneinte dies, wies die Beschwerde als unbegründet ab und führte dazu aus, dass die Finanzmarktaufsicht nicht als Empfängerin iSv Art. 4 Z 9 DSGVO gilt. Dagegen wurde Bescheidbeschwerde erhoben.

Das BVwG hat im gegenständlichen Erkenntnis die Entscheidung der DSB bestätigt und begründend ausgeführt, dass die Finanzmarktaufsicht als nach § 1 Abs. 1 FMABG eingerichtete Anstalt öffentlichen Rechts mit eigener Rechtspersönlichkeit gesetzlich zur Durchführung der Banken-, Versicherungs-, Wertpapier- und Pensionskassenaufsicht berufen ist. Sie verfügt dabei über konkrete Untersuchungsbefugnisse, wie nach § 25 Abs. 1 FM-GwG zur Überwachung der Einhaltung von Vorschriften zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung. Die Finanzmarktaufsicht ist daher berechtigt, Vor-Ort-Prüfungen bei verpflichteten Kredit- und Finanzinstituten durchzuführen. Aufgrund dieser gesetzlichen Untersuchungsbefugnisse fällt die Finanzmarktaufsicht unter die Ausnahme des Art. 4 Z 9 2. Satz DSGVO und ist nicht als „Empfänger" anzusehen. Eine Verpflichtung zur Offenlegung im Rahmen des Auskunftsrechts nach Art. 15 Abs. 1 lit. c DSGVO besteht nicht.

4. Erkenntnis des BVwG vom 20. Oktober 2025, W108 2276075-1
Datenschutzrechtliche Verantwortlichkeit bei Missachtung interner Prozesse durch Mitarbeitende
Im vorliegenden Verfahren hatte sich das BVwG mit der Frage der datenschutzrechtlichen Zurechenbarkeit von Handlungen eines Mitarbeitenden einer Organisation, der entgegen der internen Prozesse Gesundheitsdaten übermittelt hat, zu befassen.

Dem Erkenntnis vorangegangen war eine Beschwerde an die DSB wegen behaupteter Verletzung im Recht auf Geheimhaltung. Die dortige beschwerdegegnerische Partei betreibt eine Klinik. Die im Verfahren vor der DSB beschwerdeführende Partei war aufgrund des Verdachtes einer Kokainintoxikation in deren Notaufnahme aufhältig. Informationen zu diesem Aufenthalt inkl. Gesundheitsdaten wurden in weiterer Folge vom Leiter des Securitymanagements der beschwerdegegnerischen Partei unter Missachtung des diesbezüglich intern vorgegebenen Prozesses in kurzem Wege an die zuständige Landespolizeidirektion übermittelt.

Die DSB bejahte die Zurechenbarkeit des Leiters des Securitymanagements zur beschwerdegegnerischen Partei und damit deren datenschutzrechtliche Verantwortlichkeit. Die DSB gab der Beschwerde statt, zumal zwingende Bedingungen der Rechtmäßigkeit der Übermittlung von Gesundheitsdaten nicht eingehalten wurden. Gegen diese Entscheidung wurde Bescheidbeschwerde erhoben.

Das BVwG bestätigte die Ansicht der DSB und führte erläuternd aus, dass der zentrale Anknüpfungspunkt im Regime der DSGVO der Verantwortliche ist. Unter Verweis auf die Leitlinien des EDSA 07/2020 hielt das BVwG fest, dass Angestellte, die Zugriff zu personenbezogenen Daten innerhalb einer Organisation haben, grundsätzlich nicht als Verantwortliche oder als Auftragsverarbeiter zu sehen sind. In Ausnahmesituationen kann es vorkommen, dass Angestellte beschließen, personenbezogene Daten zu eigenen Zwecken zu verwenden, wodurch die erteilte Befugnis unrechtmäßig überschritten wird. Eine Organisation hat daher als Verantwortliche Sorge zu tragen, dass angemessene technische und organisatorische Maßnahmen, wie Schulungen und Informationen für Mitarbeitende, ergriffen werden, um die Einhaltung der DSGVO sicherzustellen.

Zum vorliegenden Fall hielt das BVwG fest, dass für den Krankenanstaltenbetreiber eine rechtliche Verpflichtung bestand, die Krankengeschichte aufgrund der Behandlung in der Notaufnahme zu verarbeiten. Darüber hinaus ist es gesetzlich vorgesehen, Gerichten oder Verwaltungsbehörden in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung

oder Verfügung im öffentlichen Interesse ist, auf Verlangen kostenlos Abschriften von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Patienten zu übermitteln. Für das BVwG war nicht ersichtlich, dass der Leiter des Securitymanagements die für die Verantwortlichenstellung im Sinn des Art. 4 Z 7 DSGVO ausschlaggebende Entscheidung über die Mittel und Zwecke der konkreten Datenübermittlung zu privaten Zwecken getroffen hätte. Das BVwG kommt daher zum Schluss, dass die rechtswidrige Datenübermittlung dem Klinikbetreiber zuzurechnen war und dessen datenschutzrechtliche Verantwortlichkeit gegeben war.

4.3.7.2 Beschwerdeverfahren in Verwaltungsstrafsachen

1. Erkenntnis vom 10. März 2025, W287 2286005-1

BVwG bestätigt Untersuchungsbefugnisse der DSB und Mitwirkungspflicht für Verantwortliche

Mit diesem Erkenntnis vom setzte sich das BVwG mit der Frage auseinander, inwieweit für Verantwortliche in einem Verfahren vor der DSB (z.B. Beschwerdeverfahren nach Art. 77 DSGVO) die Pflicht zur Mitwirkung, beispielsweise durch Erteilung von Auskünften besteht.

Im vorliegenden Fall hat die Verantwortliche in insgesamt fünf Beschwerdeverfahren auf zahlreiche Aufforderungen zur Stellungnahme der DSB nicht reagiert. Dadurch hat sie nach Ansicht der DSB gegen Art. 31 DSGVO verstoßen, weil sie auf Anfrage einer Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben nicht mitgewirkt hat.

Die Verantwortliche vertrat unter anderem die Ansicht, dass solche Aufforderungen der DSB lediglich der Verantwortlichen die Möglichkeit einräumen, sich am Verfahren mit einer Stellungnahme zu beteiligen (im Sinne des Parteiengehörs), aber jedenfalls keine Pflicht bestehe, eine Auskunft in Bezug auf die Beschwerde zu erteilen, weil sie sich allenfalls selbst belasten könnte (sog. Selbstbelastungsverbot - „nemo tenetur se ipsum accusare“).

Die DSB hat wegen der mangelnden Mitwirkung der Verantwortlichen sowie wegen nicht fristgerechter Befolgung einer - mit Bescheid erfolgten - Anweisung der DSB, einer betroffenen Person Auskunft nach Art. 15 DSGVO zu erteilen, eine Geldbuße in Höhe von insgesamt EUR 15.200,- verhängt.

Das BVwG beleuchtete dieses Straferkenntnis und stellte zusammengefasst Folgendes fest:

Insgesamt betrachtet legt Art. 31 DSGVO dem Verantwortlichen eine verwaltungsrechtliche Kooperationspflicht auf und die Vorschrift drängt insofern den Grundsatz der amtswegigen Sachverhaltsermittlung ein Stück weit zurück. Diese Verpflichtung ist nicht davon abhängig, ob nach Ansicht der Verantwortlichen ihre Mitwirkung zur Feststellung des Sachverhalts erforderlich ist (auch keine ex-ante-Beurteilung).

In Bezug auf das Vorbringen, das Straferkenntnis hätte die Verantwortliche in ihrem Recht sich nicht selbst belasten zu müssen verletzt, entgegnete das BVwG, dass das Selbstbelastungsverbot stets in einem Spannungsverhältnis zu einer Mitwirkungspflicht besteht. Ein solche Garantie gilt jedoch nicht absolut und kann, wie jedes andere Grundrecht auch, Einschränkungen unterworfen werden, solange der Grundkern dieses Verfahrensrecht erhalten bleibt. Mit Verweis auf die wettbewerbsrechtliche Judikatur des EuGH wird klargestellt, dass diese Garantie nicht als verletzt angesehen werde kann, solange kein unmittelbares Schuldeingeständnis verlangt wird. Diese Garantie darf jedoch nicht dazu führen, dass jegliche Zusammenarbeit mit der Aufsichtsbehörde verweigert wird. Ansonsten ist es der Behörde nicht möglich, ihre gesetzlich aufgetragenen Aufgaben zu erfüllen.

Gemessen daran folgte das BVwG der Ansicht der DSB und bestätigte das Straferkenntnis dem Grunde nach, reduzierte jedoch im Rahmen einer eigenen Ermessensentscheidung die Geldstrafe auf insgesamt EUR 10.000,- und verpflichtete die Verantwortliche zum Ersatz der Verfahrenskosten in Höhe von EUR 1.000,-.

Dem Vorbringen, dass mit einer Verwarnung das Auslangen hätte gefunden werden können, entgegnete das BVwG, dass die gänzliche Weigerung, auf Behördenschreiben zu reagieren, die Arbeit der DSB erheblich erschwert bzw. verzögert hat. Ein solches Verhalten schränkt die Wirksamkeit von Untersuchungen der DSB ein und damit auch das Allgemeininteresse an der Durchsetzbarkeit des Grundrechts auf Datenschutz. Daher folgte das BVwG der Ansicht der DSB, dass hier aus generalpräventiven Gründen die Verhängung einer entsprechenden Geldbuße erforderlich ist.

2. Erkenntnis vom 25. Juli 2025, W258 2299744-1
BVwG bestätigt die bis dato höchste Geldbuße der DSB wegen unrechtmäßiger Videoüberwachung
Mit diesem Erkenntnis vom 25 Juli 2025 setzte sich das BVwG mit der bis dato höchsten Geldbuße der DSB wegen einer unrechtmäßig betriebenen Videoüberwachungsanlage auseinander und beleuchtete dabei insbesondere die Rechtslage in Bezug auf die Frage, ob bei der Strafbemessung im Falle einer zu bestrafenden Konzerngesellschaft der gesamte Jahresumsatz des Konzerns berücksichtigt werden muss oder nur der Umsatz der einzelnen (beschuldigten) Tochtergesellschaft.

Im vorliegenden Fall verhängte die DSB mit Straferkenntnis vom 16.08.2024 eine Geldbuße in Höhe von insgesamt EUR 1,5 Millionen wegen unrechtmäßiger Datenverarbeitung durch eine überschießende Videoüberwachungsanlage von IKEA am Standort der Filiale Wien Westbahnhof. Gegenstand waren mehrere Innen- und Außenkameras der Filiale, die über einen Zeitraum von mehreren Monaten personenbezogene Bilddaten – teils auch PIN-Eingaben bei Selbstbedienungskassen – erfassten und speicherten, obwohl dies für die genannten Zwecke nicht erforderlich war.

IKEA erhob dagegen eine Beschwerde an das BVwG und führte unter anderem ins Treffen, dass der Konzernumsatz von IKEA bei der Strafbemessung nicht berücksichtigt werden dürfe, sondern nur der (deutlich niedrigere) Umsatz des einzelnen Einrichtungshauses, das neu errichtet worden sei. Die DSB verwies auf das Urteil des EuGH vom 13.02.2025, C-383/23, „[ILVA]“ und entgegnete, dass bei der Strafbemessung die tatsächliche wirtschaftliche Leistungsfähigkeit eines Unternehmens berücksichtigt werden muss und daher im Zusammenhang mit der Unternehmensgröße auch zu berücksichtigen ist, ob die Beschuldigte einem Konzern angehört.

Das BVwG folgte im Ergebnis der Ansicht der DSB und stellte fest, dass das Vorbringen von IKEA keine Deckung im Wortlaut des Art. 83 DSGVO findet und dem Urteil des EuGH widerspricht. Die DSB muss bei der Verhängung von Geldbußen sicherstellen, dass diese in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sind. Hierbei muss unter anderem auch geprüft werden, ob der Adressat der Geldbuße einem Konzern angehört.

Im Ergebnis können Verstöße gegen die Sorgfaltspflichten im Rahmen der Eröffnung eines (weiteren) Standortes nur wirksam und abschreckend geahndet werden, wenn bei der Bestimmung der Geldbuße auf die wirtschaftliche Situation der Konzernmutter abgestellt wird, weil es letztlich an ihr liegt, sicherzustellen, dass bei zukünftigen Eröffnungen eines Standortes datenschutzrechtlichen Vorgaben die angemessene Sorgfalt gewährt wird.

IKEA hat eine Revision gegen das Erkenntnis des BVwG eingebracht und das BVwG hat die aufschiebende Wirkung für die Bezahlung der Geldstrafe gewährt. Die Verwaltungsstrafsache ist nun

beim VwGH anhängig. Die DSB hat eine Revisionsbeantwortung eingebracht sowie einen Antrag an den VwGH gestellt, der Revision die aufschiebende Wirkung abzuerkennen.

3. Erkenntnis vom 27. Februar 2025, W298 2305443-1
Auskunftspflicht nach Art. 15 DSGVO besteht unabhängig von der genannten Rechtsgrundlage
Das BVwG bestätigte ein Straferkenntnis der DSB gegen einen Rechtsanwalt wegen Nichtbeantwortung eines Auskunftsbegehrens. Die betroffene Person hatte ihr Begehren formal als „Antrag gemäß § 44 DSG" bezeichnet, obwohl diese Bestimmung nur für Datenverarbeitungen nach dem 3. Hauptstück des DSG gilt. Der Rechtsanwalt verweigerte daraufhin die Auskunft mit der Begründung, es liege kein zulässiger Auskunftsantrag nach Art. 15 DSGVO vor.

Die DSB widersprach dem Verantwortlichen und verhängte wegen der verweigerten Auskunft eine Geldbuße in Höhe von EUR 400,-. Dagegen brachte der Verantwortliche eine Beschwerde ein und das BVwG setzte sich näher mit den Pflichten nach Art. 15 DSGVO auseinander:

Das BVwG stellte klar, dass das Auskunftsrecht nach Art. 15 DSGVO an keinerlei Formvorschriften gebunden ist. Maßgeblich sei allein, ob aus dem Begehren objektiv erkennbar hervorgeht, dass eine betroffene Person Auskunft über die Verarbeitung ihrer personenbezogenen Daten verlangt. Die falsche Bezeichnung der Rechtsgrundlage oder die Verwendung eines unzutreffenden Formulars entbinde den Verantwortlichen nicht von seiner Pflicht zur Reaktion („falsa demonstratio non nocet")

Selbst wenn aufgrund berufsrechtlicher Verschwiegenheitspflichten (hier: § 9 RAO) inhaltlich keine oder nur eingeschränkte Auskunft erteilt werden dürfe, bestehe jedenfalls eine Reaktions- und Informationspflicht, etwa durch eine (teilweise) Auskunft oder eine begründete Ablehnung. Das völlige Untätigbleiben stelle jedenfalls eine Verletzung der Art. 12 und 15 DSGVO dar. Es wird darauf hingewiesen, dass nach § 9 Abs. 4 RAO keine gänzliche Ausnahme von der Auskunftspflicht normiert wird.

Hinsichtlich der Strafbemessung bestätigte das BVwG die Geldbuße zur Gänze. Es wertete den Verstoß als vorsätzlich, da der Beschwerdeführer trotz ausdrücklicher Hinweise der DSB auf seine Auskunftspflicht nicht reagierte. Strafmildernd berücksichtigte das Gericht das Fehlen einschlägiger Vorstrafen und die Kooperation im Verfahren vor dem BVwG.

4.3.8 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 Art. 33 DSGVO **1704 nationale Sicherheitsverletzungen („Data Breaches")** gemeldet.

Dazu kamen **48 Meldungen betreffend grenzüberschreitende Sicherheitsverletzungen** sowie **20 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 **83 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.

Damit hat sich die Anzahl der im Berichtszeitraum für das Jahr 2025 insgesamt bei der Datenschutzbehörde eingelangten Meldungen von Sicherheitsverletzungen im Vergleich zum Vorjahr von insgesamt 1319 auf **1855 wesentlich erhöht**.

Auch im Jahr 2025 betraf eine wesentliche Anzahl der gemeldeten Vorfälle **Hackerangriffe** auf Unternehmen oder sonstige Einrichtungen, darunter unzählige unterschiedliche **Ransomware-Attacken** mit dem Ziel der Verschlüsselung von Daten, deren Übermittlung an die Angreifer:innen bzw. der Offenlegung der gehackten Datensätze im Darknet. Davon betroffen waren u.a. Buchungsplattformen und Lohnverrechnungs- und Personalverwaltungs-Softwareprogramme.

Weiters konnte eine Häufung von Sicherheitsverletzungen beobachtet werden, die aufgrund von **(fahrlässigem) menschlichen Verhalten** verursacht wurden. So wurden etwa Dokumente oder sonstige Unterlagen (wie etwa Kontoauszüge, Versicherungsunterlagen, Kaufverträge, Patientenakten) an falsche Empfänger:innen übermittelt. Dies erfolgte sowohl (meistens) per E-Mail als auch per Postversand oder durch persönliche Übergabe. Auch die unsachgemäße Entsorgung/Vernichtung von Unterlagen wurde mehrfach gemeldet.

Daneben kam es immer wieder zu **bewusst gesetzten Handlungen von Mitarbeiter:innen** bestimmter Unternehmen bzw. Institutionen mit dem Ziel der Veröffentlichung von Daten in sozialen Medien. So wurden etwa Bestandteile von Patientenakten oder Patientenfotos im Internet gepostet. Auch der Zugriff auf personenbezogene Daten von Kolleg:innen oder Kund:innen aus reiner Neugier (oder aufgrund einer sonstigen Motivation heraus) war wiederholt Thema von Meldungen nach Art. 33 DSGVO.

Ebenso wurde auch wieder eine Vielzahl von Sicherheitsverletzungen aufgrund **technischer Fehler oder organisatorischer Mängel**, welche unerwünschte Offenlegungen an fremde Personen zur Folge hatten, gemeldet (falsche Verknüpfungen von Konten oder User-Accounts, falsche Kontostände, doppelt durchgeführte Überweisungen, Vergabe falscher Zugriffsberechtigungen etc.).

In all den oben genannten Fällen hat die:der Verantwortliche schnellstmöglich Maßnahmen zu ergreifen, die zur Reduzierung des Risikos führen. Dazu zählen beispielsweise im Falle von Ransomware 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 neben einem **PDF-Formular** auch ein **Onlineformular** zur Verfügung.

Diese Formulare finden sich unter:

https://dsb.gv.at/eingabe-an-die-dsb/-meldung-data-breach

4.3.9 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 die:der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, die beabsichtigte Verarbeitung ein hohes Risiko zur Folge hätte, hat die:der Verantwortliche die Aufsichtsbehörde zu konsultieren.

Im Rahmen dieses Konsultationsverfahrens gemäß **Art. 36 DSGVO** hat die Aufsichtsbehörde verschiedene Befugnisse. Sie kann etwa der:dem Verantwortlichen bzw. der:dem Auftragsverarbeiter:in **schriftliche Empfehlungen** unterbreiten, sofern sie der Ansicht ist, dass die geplante Verarbeitung nicht im Einklang mit der DSGVO steht, etwa, weil die:der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat. Darüber hinaus kann die Aufsichtsbehörde sämtliche in **Art. 58 DSGVO** genannten Befugnisse ausüben.

Im Jahr 2025 wurde die DSB als Aufsichtsbehörde in **keinem Fall gemäß Art. 36 DSGVO** konsultiert.

4.3.10 Anträge auf Genehmigung von Verhaltensregeln und Zertifizierungskriterien

4.3.10.1 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 sieben dieser Verhaltensregeln wurde bereits eine **dazugehörige Überwachungsstelle gemäß Art. 41 Abs. 2 DSGVO akkreditiert.**

Eine **Übersicht** findet sich auf der **Website der DSB**.[27] Darüber hinaus hat auch der **EDSA ein Register** von Verhaltensregeln aller Mitgliedstaaten veröffentlicht, welches laufend ergänzt wird.[28]

27 https://dsb.gv.at/ueber-die-datenschutzbehoerde/verhaltensregeln, abgerufen am 18.02.2026.
28 https://dsb.gv.at/ueber-die-datenschutzbehoerde/verhaltensregeln, abgerufen am 18.02.2026.

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

4.3.10.2 Zertifizierungskriterien

Verantwortliche oder Auftragsverarbeiter:innen können von akkreditierten Zertifizierungsstellen die Erteilung einer **datenschutzrechtlichen Zertifizierung** gemäß Art. 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 **Erwägungsgrund 100 der DSGVO** soll durch Zertifizierungen die Transparenz im Zusammenhang mit der Verarbeitung personenbezogener Daten erhöht und die Einhaltung der DSGVO verbessert werden.

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

Die DSB hat mit Bescheid vom 7. August 2025, OZ: 2025-0.623.800 (GZ: D163.009), die **zweiten nationalen datenschutzrechtlichen Zertifizierungskriterien gemäß Art. 42 Abs. 5 DSGVO genehmigt**. Die zugehörige Zertifizierungsstelle wurde bereits (unter aufschiebender Bedingung) mit Bescheid vom 23. September 2024, GZ: 2024-0.623.629, akkreditiert.

Auf der Website der DSB finden sich ein **Verzeichnis der akkreditierten Zertifizierungsstellen**[29] sowie weitere Informationen zum Thema Zertifizierungen.

4.3.11 Verwaltungsstrafverfahren

Die DSB ist gemäß **§ 22 Abs. 5 DSG** als nationale Aufsichtsbehörde für die **Verhängung von Geldbußen gemäß Art. 58 Abs. 2 lit. i DSGVO** für Verstöße gegen die bußgeldbewehrten Bestimmungen nach **Art. 83 DSGVO** und **subsidiär § 62 DSG** sowohl gegenüber **natürlichen als auch juristischen Personen** zuständig. Die Strafkompetenz der DSB wird zudem durch weitere Rechtsakte erweitert (siehe hierzu die **Kapitel 8., 9. und 11.**).

Diese Aufgaben werden innerhalb der DSB von der Abteilung V wahrgenommen.

Die DSB hat im Berichtszeitraum 2025 im Rahmen von Verwaltungsstrafverfahren insgesamt 75 Bescheide erlassen, davon **58** in Form von **Geldbußen** mit einer Gesamtsumme von rund **EUR 145.000**,-.

29 https://dsb.gv.at/ueber-die-datenschutzbehoerde/verzeichnis-der-akkreditierten-zertifizierungsstellen-zertifizierungsvoraussetzungen, abgerufen am 18.02.2026.

Insgesamt wurden **10 Strafbescheide mittels Beschwerde bekämpft**. Der überwiegende Teil der ausgesprochenen Geldstrafen wurde somit nicht angefochten.

Im Übrigen wurden im Berichtszeitraum neben den 127 eingeleiteten Verfahren **85 Fälle zur Einstellung gebracht** (in 26 Fällen erfolgte die Einstellung des Verfahrens zusammen mit einem verfahrensbeendenden Sensibilisierungsschreiben).

Folgende Entscheidungen bzw. Strafbescheide sind im Berichtszeitraum hervorzuheben:

1. Straferkenntnis vom 20. Jänner 2025, OZ: 2024-0.832.169 (GZ: D550.934)
Unrechtmäßige Videoüberwachungsanlage zum Zwecke der Besucherstromanalyse
Die DSB hat mit Straferkenntnis vom 20. Jänner 2025 eine Strafe in Höhe von EUR 21.120,- ausgesprochen.

Die Beschuldigte hat in einem Zeitraum von knapp drei Jahren unrechtmäßig personenbezogene Daten verarbeitet, indem diese innerhalb einer gut besuchten Innenstadt eine Videoüberwachungsanlage, bestehend aus insgesamt 27 Videokameras, betrieben hat. Die Kameras waren hierbei jeweils an den Zutrittsbereichen der Innenstadt montiert. Durch die Aufnahmebereiche der Kameras wurden regelmäßig personenbezogenen Daten verarbeitet, bspw. durch Erfassen von Passant:innen und KFZ- Kennzeichen. Die Kameras nahmen in Echtzeit 24 Stunden am Tag auf und generierten digitales Bildmaterial, welches in textuelle Daten zum Zwecke der Besucherstromanalyse bzw. Frequenzanalyse umgewandelt wurde, um Informationen für die Bewertung von Auslastungen dieser Plätze zu gewinnen und diese als Indikatoren für die Planung, Organisation und Durchführung von Events bzw. Veranstaltungen zu verwenden.

Die dabei erfolgte Verarbeitung in Form der Erhebung personenbezogener (Bild-)Daten konnte auf keine Rechtsgrundlage nach Art. 6 Abs. 1 iVm Art. 5 Abs. 1 lit. a DSGVO gestützt werden und erfolgte entgegen dem Grundsatz der Datenminimierung im Sinne des Art. 5 Abs. 1 lit. c DSGVO, zumal weniger eingriffsintensive Zähltechniken zur Personen- bzw. Frequenzmessung zur Verfügung stehen.

Zudem hat die Beschuldigte gegen Art. 12 und Art. 13 DSGVO verstoßen, indem keine der 27 Videokameras gekennzeichnet war und auch sonst nicht auf die vorgenommene Bildverarbeitung hingewiesen wurde.

Der Schuldspruch des Straferkenntnisses wurde vom BVwG in dessen Erkenntnis vom 11. Juni 2025, W211 2308914-1, bestätigt, die Strafhöhe jedoch reduziert.

2. Straferkenntnis vom 16. April 2025, OZ: 2025-0.109.181 (GZ: D550.1039)
Unrechtmäßige Entsorgung von Gästebüchern in Papierkübeln
Die DSB hat mit Straferkenntnis vom 16. April 2025 eine Strafe in Höhe von EUR 600,- ausgesprochen, da der Beschuldigte mehrere Gästebücher einer Pension, welche zumindest Name, Hauptwohnsitz, Ehegatte, Geburtsdatum, Reisezeitraum von zahlreichen Gästen enthielten, in mindestens zwei unversperrten Papierkübeln, die an der Straßenfront zur Abholung bereitstanden entsorgt hatte. Die in den Papierkübeln enthaltenen Dokumente waren für Dritte, konkret: Passant:innen, ohne Weiteres einsehbar.

Die dabei erfolgte Verarbeitung der im Dateisystem „Gästebuch“ erfassten personenbezogenen Daten in Form der Entsorgung sowie die dadurch bewirkte Offenlegung konnten auf keine Rechtsgrundlage gemäß Art. 6 Abs. 1 in Verbindung mit Art. 5 Abs. 1 lit. a DSGVO gestützt werden und erfolgten zudem entgegen dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO.

Zudem hat der Beschuldigte gegen den Grundsatz der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f DSGVO und seine Pflicht gemäß Art. 32 DSGVO verstoßen.

Das Straferkenntnis ist rechtskräftig.

3. Straferkenntnis vom 4. August 2015, OZ: 2025-0.613.487 (D550.1177)
Unrechtmäßige Offenlegung des Patientenstammes
Die DSB hat mit Straferkenntnis vom 4. August 2025 eine Strafe in Höhe von EUR 4.000,- ausgesprochen.

Der Beschuldigte verwendete die elektronischen Kontaktdaten – konkret die E-Mail-Adressen seines Patientenstamms sowie seiner Geschäftspartner:innen – aus seinen Ordinationen, um über das E-Mail-System einer GmbH, bei welcher er seit kurzem als ärztlicher Leiter tätig war, ein E-Mail zur Erweiterung seiner medizinischen Tätigkeit zu versenden.

Durch die Weitergabe der E-Mail-Adressen an eine Dritte kam es zu einer unzulässigen Offenlegung personenbezogener Daten, die weder erforderlich noch für die Betroffenen vorhersehbar war. Mangels eines Erlaubnistatbestands gemäß Art. 6 Abs. 1 in Verbindung mit Art. 9 Abs. 2 DSGVO stellte dies eine unrechtmäßige Verarbeitung und einen Verstoß gegen Art. 5 Abs. 1 lit. a sowie lit. c DSGVO dar.

Das Straferkenntnis ist rechtskräftig.

4. Straferkenntnis vom 6. August 2025, OZ: 2025-0.276.820 (GZ: D550.1173)
Nichtbefolgung einer Anweisung der Datenschutzbehörde
Die DSB hat mit Straferkenntnis vom 06. August 2025 eine Strafe in Höhe von EUR 6.200,- ausgesprochen, da die Beschuldigte eine Anweisung der DSB nach Art. 58 Abs. 2 lit. d DSGVO missachtet hatte.

Konkret hatte die Beschuldigte das datenschutzrechtliche Ersuchen um Einwilligung (den sogenannten „Cookie-Banner“) auf ihrer Website derart abzuändern, dass auf der ersten Ebene des Cookie-Banners zusätzlich zur Option „Akzeptieren“ eine optisch gleichwertige Option vorgesehen ist, mit der der Cookie-Banner ohne Abgabe einer Einwilligung geschlossen werden kann. Dieser Anweisung kam die Beschuldigte jedoch erst weit nach Ablauf der Leistungsfrist nach.

Das Straferkenntnis ist rechtskräftig.

5. Straferkenntnis vom 8. August 2025, OZ: 2025-0.566.040 (GZ: D550.1172)
Unrechtmäßige Videoüberwachung in Arztpraxis
Die DSB hat mit Straferkenntnis vom 8. August 2025 eine Strafe in Höhe von EUR 1.000,- ausgesprochen.

Der Beschuldigte hatte in seiner Kassenordination für Allgemeinmedizin sowie Privatordination für Orthopädie und Unfallchirurgie jedenfalls für einen Zeitraum von über zwei Jahren eine Videoüberwachungsanlage bestehend aus fünf Videoüberwachungskameras im Bereich der Verkehrswege, nämlich im Eingangs-, Warte- und Infusionsbereich, installiert. Die Anlage diente dem Schutz des Lebens, der Gesundheit und der körperlichen Unversehrtheit von Personen sowie dem Schutz des Eigentums, zumal es bereits in der Vergangenheit dazu gekommen ist, dass Patient:innen im Warte- und Infusionsbereich kollabiert sind und sich bereits Personen Zugang zu medizinischem Material verschafft haben.

Die Kameras erfassten in den Ordinationsräumlichkeiten regelmäßig Mitarbeiter:innen sowie Patient:innen bzw. Begleitpersonen. Die DSB hatte daher zwischen den Betroffenenkreisen und zwischen sensiblen und nicht sensiblen personenbezogenen Daten zu differenzieren:

Für die Verarbeitung der personenbezogenen Daten der Mitarbeiter:innen war weder Art. 6 Abs. 1 lit. a DSGVO noch Art. 6 Abs. 1 lit. f DSGVO einschlägig, zumal – wenngleich eine Einverständniserklärung nach § 10 AVRAG vorlag – keine Einwilligung im Sinne der DSGVO bestand und nicht erkennbar war, weshalb zur Erreichung der ins Treffen geführten berechtigten Interessen eine durchgehende/permanente Überwachung des Eingangs-, Warte- und Infusionsbereiches erforderlich scheint. Zweiteres lässt sich auch auf die Begleitpersonen übertragen.

Hinsichtlich der Patienten und Patientinnen kann jedenfalls – entgegen der Ansicht des Beschuldigten – nicht gesagt werden, dass die Videoüberwachungsanlage für die Zwecke des Behandlungsvertrages als unbedingt erforderlich angesehen werden kann, zumal diese auch nicht für einen bestimmten Anlassfall erfolgt, sondern vielmehr präventiv für potentielle Einsätze. Im Übrigen lässt sich weder aus § 49 noch aus § 51 ÄrzteG eine direkte Verpflichtung zur Verarbeitung von Patient:innendaten mittels Videoüberwachungsanlage ableiten oder ergibt sich eine Dokumentationspflicht, für welche eine Videoüberwachungsanlage erforderlich wäre. Demnach ließ sich weder aus dem Behandlungsvertrag noch einer gesetzlichen Grundlage eine Rechtfertigung nach Art. 9 Abs. 2 lit. h DSGVO ableiten. Auch kommt eine Rechtfertigung nach Art. 9 Abs. 1 lit. c DSGVO aufgrund lebenswichtiger Interessen der betroffenen Personen nicht in Betracht, da die Verarbeitung bereits zu einem Zeitpunkt einsetzte, zu dem der:die Patient:in noch bei Bewusstsein war – nämlich bei der Aufnahme bzw. Anmeldung in den Ordinationsräumlichkeiten –, "Daher wäre es diesem:dieser durchaus zumutbar, ausdrücklich in die Verarbeitung durch Videoüberwachung einzuwilligen.

Das Straferkenntnis ist rechtskräftig.

6. Straferkentnnis vom 4. September OZ: 2025-0.699.550 (GZ: D550.1221)
Verspätete Meldung einer Sicherheitsverletzung
Die DSB hat mit Straferkenntnis vom 04. September 2025 eine Strafe in Höhe von EUR 870,- aufgrund einer verspäteten Meldung einer Sicherheitsverletzung ausgesprochen.

Nach Art. 33 Abs. 1 DSGVO müssen Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten den Vorfall unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde melden.

Die DSB sprach in diesem Zusammenhang aus, dass auch eine Nachricht, welche intern von der Beschuldigten zwar als Spam-Nachricht eingestuft wurde als Kenntnisnahme der Sicherheitsverletzung und sohin als fristauslösendes Ereignis zählt.

Das Straferkenntnis ist rechtskräftig.

7. Straferkenntnis vom 5. September 2025 OZ: 2025-0.661.437 (GZ: D550.1166)
Unrechtmäßige Videoüberwachungskameras in Bäckereien
Die DSB hat mit Straferkenntnis vom 5. September 2025 eine Strafe in Höhe von EUR 33.500,- ausgesprochen.

Die Beschuldigte betrieb zum Schutz der Mitarbeiter:innen, der Kassen sowie zum Schutz vor Einbrüchen über einen Zeitraum von mehr als einem Jahr an mehreren Standorten ihrer Bäckereien insgesamt 30 unzureichend gekennzeichnete Videokameras. Die Kameras befanden sich

sowohl im Kundenbereich, als auch in Bereichen, welche ausschließlich von Mitarbeiter:innen genutzt wurden.

Die Kameraeinstellungen entsprachen weder zeitlich noch örtlich dem gelindesten Mittel. So wurden teilweise öffentliche Bereiche oder reine Kundenbereiche gefilmt. Außerdem waren die Kameras abseits jener Bereiche, die für Kunden erreichbar waren, auch in Zeiten aktiv, in welcher bereits bzw. noch Mitarbeiter:innen zugegen waren, zB Bäcker:innen, die in den frühen Morgenstunden ihren Dienst verrichteten oder Reinigungskräfte, die nach den Öffnungszeiten ihren Aufgaben nachgingen.

Die Videoüberwachungsanlage erfasste in ihrer Gesamtheit daher unter anderem regelmäßig Passant:innen, Kund:innen sowie Mitarbeiter:innen ohne Vorliegen einer die Verarbeitungen rechtfertigenden Bedingung und lag daher eine Verletzung des Art. 5 Abs. 1 lit. a und c sowie Art. 6 Abs. 1 DSGVO vor.

Zudem wurden zumindest in einem Fall Aufnahmen unrechtmäßig entgegen Art. 6 Abs. 4 DSGVO weiterverarbeitet. Die Bilddaten aus einer der Anlagen wurden – entgegen dem festgelegten Zweck - in einer Messengerdienst-Gruppe mit Führungskräften geteilt. Die Aufzeichnung zeigte einen Arbeitnehmer bei der Verrichtung seiner Tätigkeit und die Aufnahme wurde versendet, weil man mit der Arbeitsleistung des Arbeitnehmers zum aufgenommenen Zeitpunkt nicht zufrieden war.

Das Straferkenntnis ist nicht rechtskräftig.

8. Straferkenntnis vom 8. September 2025 OZ: 2025-0.388.125 (GZ: D550.1202) Unrechtmäßige Aufzeichnung eines Vertragsgespräches

Die DSB hat mit Straferkenntnis vom 8. September 2025 eine Strafe in Höhe von EUR 6.300,- ausgesprochen.

Die Beschuldigte hat durch ihren Geschäftsführer während der Öffnungszeiten in einer Ordination im Zuge eines Termins zum Abschluss eines Vertrags über elektronische Medien ein Gespräch mit einer dort angestellten Ärztin heimlich mittels eines Aufnahmegeräts aufgezeichnet. Inhalt des Gespräches war eine Dienstleistung in Form einer App, auf welcher Informationen zu Betrieben und Gewerben innerhalb eines Bundeslandes abgerufen werden können. Die Aufzeichnung erfasste neben dem Gesprächsinhalt unter anderem die E-Mail-Adresse und den Namen der Gesprächspartnerin, die Namen der Instagram- und Facebook-Accounts der Ordination sowie Informationen zur Ausbildung der die Ordination innehabenden Ärztin. Die Gesprächspartnerin wurde erst im laufenden Gespräch über die bereits erfolgende Aufzeichnung informiert.

Aufgrund der Tatsache, dass die Audioaufnahme durch die Beschuldigte bereits vor Betreten des Tatortes gestartet wurde, war das Einholen einer datenschutzrechtlichen Einwilligung – entgegen der Ansicht der Beschuldigten – vor Beginn der Verarbeitung faktisch unmöglich.

Die Beschuldigte gab im Übrigen einerseits die Verarbeitung zu Qualitätszwecken als auch die Nutzung der Aufzeichnung für Beweiszwecke an. Sowohl die Qualitätssicherung als auch die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen stellen grundsätzlich berechtigte Interessen dar.

Im Hinblick auf die Verarbeitung zu Beweiszwecken schied das berechtigte Interesse der Beschuldigten jedoch aus, da die Beschuldigte zur Tatzeit unmöglich davon ausgehen hätte können, dass sie zu einem späteren Zeitpunkt die Aufnahme in einem straf- oder zivilgerichtlichen Verfahren

zu Beweiszwecken benötigen würde, vielmehr käme dieses Verhalten einer unzulässigen Vorratsdatenspeicherung gleich.

Hinsichtlich der Qualitätssicherung schied die Berufung auf berechtigten Interessen ebenso aus, da die Beschuldigte die Betroffenen nicht vor Erhebung ihrer Daten über die berechtigten Interessen informiert hatte, vielmehr erfolgte dies erst als die Verarbeitung bereits im Gang war.

Die Aufzeichnung erfolgte ohne entsprechende Rechtsgrundlage nach Art. 5 Abs. 1 lit. a iVm Art. 6 Abs. 1 DSGVO und entgegen dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO.

Das Straferkenntnis ist nicht rechtskräftig.

9. Straferkenntnis vom 7. Oktober OZ: 2025-0.778.661 (GZ: D550.1230)
Unrechtmäßige Einsichtnahme in eine private Festplatte einer Arbeitskollegin
Die DSB hat mit Straferkenntnis vom 07. Oktober 2025 eine Strafe in Höhe von 2.500 EUR ausgesprochen.

Der Beschuldigte, amtierender Polizeibeamter, hat sich mittels Ersatzschlüssel Zugang zu einer versperrten Festplatte seiner Arbeitskollegin verschafft und diese an den zur Datenauswertung bestimmten Computer angesteckt und Bild(-Daten) der Betroffenen (in Bekleidung und in Unterwäsche, als auch beim Stillen) eingesehen.

Die Verarbeitung erfolgte ohne eine die Verarbeitung rechtfertigende Bedingung nach Art. 5 Abs. 1 lit. a iVm Art. 6 Abs. 1 DSGVO sowie ohne legitimen Zweck gemäß Art. 5 Abs. 1 lit. b DSGVO.

Bei der Bemessung der Strafhöhe war zu berücksichtigen, dass gegenüber dem Beamten eine Suspendierung sowie eine hohe Geldstrafe im Rahmen eines Disziplinarverfahrens verhängt worden waren. Der Beschuldigte legte ein reumütiges Geständnis ab, war einsichtig und kooperierte im vollen Umfang mit der DSB.

Das Straferkenntnis ist rechtskräftig.

10. Straferkenntnis vom 7. Oktober 2025 OZ: 2025-0.811.087 (GZ: D550.1224)
Veröffentlichung von Strafdaten über Facebook
Die DSB hat mit Straferkenntnis vom 7. Oktober 2025 eine Strafe in Höhe von EUR 2.500,- ausgesprochen.

Die Beschuldigte fertigte mithilfe einer Videoüberwachungsanlage mit unzulässig weit gefasstem Aufnahmebereich zwei Lichtbildaufnahmen an und veröffentlichte diese über ihr öffentlich zugängliches Facebook-Profil zur Fahndung nach der auf den Lichtbildaufnahmen abgebildeten, der Polizei bekannten Person.

Die DSB sprach in diesem Zusammenhang unter anderem aus, dass der Beitrag Informationen enthält, die eine Person als mutmaßlichen Täter einer Straftat identifizieren und als Strafdaten im Sinne des Art. 10 DSGVO zu qualifizieren sind.

Zwar liegt es in der Natur der Sache, dass Videoaufzeichnungen, die Personen zeigen, welche in das Eigentum anderer eingreifen, zur Ermittlung etwaiger Straftaten herangezogen werden können. Die Weiterverarbeitung der Lichtbildaufnahmen erfolgte dennoch zweckwidrig, da die Veröffentlichung der Aufnahmen über ein öffentlich zugängliches Facebook-Profil einer öffentlichen Fahndung gleichkommt, die für die betroffene Person weder nachvollziehbar noch vorhersehbar

ist. Auch die Folgen der Weiterverarbeitung waren nicht zu unterschätzen. Weiters lag für die zweckändernde Weiterverarbeitung weder eine Einwilligung noch eine entsprechende nationale Rechtsgrundlage im Sinne des Art. 6 Abs. 4 DSGVO vor. Die Weiterverarbeitung erwies sich folglich nach durchgeführtem Kompatibilitätstest als zweckwidrig.

Das Straferkenntnis ist rechtskräftig.

4.3.12 Stellungnahmen zu Gesetzes- und Verordnungsvorhaben

Die DSB hat im Jahr 2025 zu folgenden Vorhaben **eine Stellungnahme** abgegeben. Die Stellungnahmen sind, soweit es sich nicht um jene zu Verordnungen oder Landesgesetzen handelt, unter www.parlament.gv.at abrufbar.

1. Landesgesetz, mit dem das Gesetz über die Einrichtung und die Aufgaben der Feuerwehr im Lande Wien (Wiener Feuerwehrgesetz) geändert wird

2. Verordnung, mit der die Verordnung über die Freiwilligen Feuerwehren und die Betriebsfeuerwehren im Lande Wien (Wiener Feuerwehr-Verordnung) geändert wird

3. Landesgesetz, mit dem die Geschäftsordnung des Tiroler Landtages 2015 geändert wird

4. Landesgesetz über die aufgrund der Einführung einer allgemeinen Informationsfreiheit erforderliche Anpassung der Tiroler Landesrechtsordnung (Tiroler Informationsfreiheits Anpassungsgesetz)

5. Entwurf eines Landesgesetzes, mit dem das Wiener Fördertransparenzgesetz, das Wiener Akademienförderungsgesetz 2024 und das Wiener Parteienförderungsgesetz 2013 geändert werden sollen (Fördertransparenzpaket 2025)

6. Bundesgesetz, mit dem das Universitätsgesetz 2002 und das Bildungsdokumentationsgesetz 2020 geändert werden

7. Oberösterreichisches Informationsfreiheits-Anpassungsgesetz (Oö. IFAG)

8. Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienst-Gesetz, das Sicherheitspolizeigesetz, das Telekommunikationsgesetz 2021, Bundesverwaltungsgerichtsgesetz und das Richter- und Staatsanwaltschaftsdienstgesetz geändert werden

9. Bundesgesetz, mit dem das Arbeits- und Sozialgerichtsgesetz, das Außerstreitgesetz, das Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union, das Datenschutzgesetz, das Disziplinarstatut für Rechtsanwälte und Rechtsanwaltsanwärter, das Jugendgerichtsgesetz, die Jurisdiktionsnorm, die Notariatsordnung, die Rechtsanwaltsordnung, das Rechtspraktikantengesetz, das Staatsanwaltschaftsgesetz, das Strafgesetzbuch, die Strafprozessordnung und die Zivilprozessordnung geändert werden (IFG-Anpassungsgesetz-Justiz – IFG-AnpJu)

10. Bundesgesetzes, mit dem das Wehrgesetz 2001, das Heeresdisziplinargesetz 2014 und das Militärbefugnisgesetz geändert werden (als Teil der Vorbereitung des Gesetzespakets "Informationsfreiheit")

11. Bundesgesetz zur Digitalisierung der CEMT-Genehmigungen

12. Bundesgesetz, mit dem ein Bundesgesetz zur Regelung der Elektrizitätswirtschaft (Elektrizitätswirtschaftsgesetz – ElWG) und ein Bundesgesetz zur Definition des Begriffs der Energiearmut für die statistische Erfassung und für die Bestimmung von Zielgruppen für Unterstützungsmaßnahmen (Energiearmuts-Definitions-Gesetz – EnDG) erlassen sowie das Energie-Control-Gesetz geändert werden

13. Bundesgesetz, mit dem das Allgemeine Bürgerliche Gesetzbuch, das Arbeitsvertragsrechts-Anpassungsgesetz und das Landarbeitsgesetz 2021 geändert werden

14. Bundesgesetz, mit dem das Allgemeine Sozialversicherungsgesetz und das Arbeitsvertragsrechts-Anpassungsgesetz geändert werden

15. Bundesgesetz, mit dem das Gesundheitstelematikgesetz 2012 und das Allgemeine Sozialversicherungsgesetz geändert werden

16. Bundesgesetz, mit dem das Lebensmittelbewirtschaftungsgesetz 1997 geändert wird

17. Entwurf eines NÖ Fördertransparenzgesetzes 2025 (NÖ FTG 2025)

18. Bundesgesetz, mit dem das Waffengesetz 1996 geändert wird

19. Bundesgesetz, mit dem ein Bundesgesetz über die Beschleunigung des Ausbaus von Anlagen zur Erzeugung von Energie aus erneuerbaren Quellen, deren Speicherung und Verteilung (Erneuerbaren-Ausbau-Beschleunigungsgesetz – EABG) erlassen sowie das Erneuerbaren-Ausbau-Gesetz geändert wird

20. Bundesgesetz, mit dem das Politische-Werbung-Gesetz erlassen und das KommAustria-Gesetz sowie das Mediengesetz geändert wird

21. Bundesgesetz, mit dem das IVS-Gesetz geändert wird

22. Bundesgesetz, mit dem das Schulunterrichtsgesetz, das Pflichtschulerhaltungs-Grundsatzgesetz und das Schulpflichtgesetz 1985 geändert werden

23. Bundesgesetz, mit dem die Straßenverkehrsordnung, das Kraftfahrgesetz 1967 und das Führerscheingesetz geändert werden (36. Novelle der Straßenverkehrsordnung)

24. Bundesgesetz, mit dem das Bundesgesetz über die Dokumentation im Gesundheitswesen geändert wird (DokuG-Novelle 2025)

25. Bundesgesetz, mit dem das Eltern-Kind-Pass-Gesetz, das Kinderbetreuungsgeldgesetz und das Familienlastenausgleichsgesetz 1967 geändert werden

26. Bundesgesetz, mit dem das Bundespflegegeldgesetz geändert wird

27. Entwurf der Zweiten Transparenzdatenbank-Abfrageverordnung 2025

28. Bundesgesetz über die Einführung einer Beleglotterie (Beleglotteriegesetz)

5. Wesentliche höchstgerichtliche Entscheidungen

5.1 Verfassungsgerichtshof - VfGH

Der VfGH hat im Berichtszeitraum[30] 2025 **9** veröffentlichte **datenschutzrechtliche Entscheidungen** getroffen. Er hat sich dabei im Berichtszeitraum bereits mehrfach mit Beschwerden befasst, bei deren Entscheidung zwischen Vorschriften im Dienste der Transparenz und Informationsfreiheit (Art. 10 EMRK; Art. 22a B-VG und das IFG selbst sind erst am 1. September 2025 in Kraft getreten) und dem Grundrecht auf Datenschutz (insbesondere gemäß § 1 DSG) abzuwägen war[31]. Ein Antrag des BVwG, eine (bereits außer Kraft getretene) Transparenzbestimmung im PartG als verfassungswidrig aufzuheben[32], wurde zurückgewiesen[33].

Weiters hat der VfGH in einem Verfahren, das bei der DSB seinen Ausgang genommen hat, die verfassungsrechtliche Prüfung einer Beschwerde betreffend eine gemäß Art. 83 DSGVO gegen eine juristische Person verhängte Geldbuße gemäß Art. 144 Abs. 2 B-VG abgelehnt und dabei u.a. auf den fehlenden Umsetzungsspielraum des nationalen Gesetzgebers verwiesen.[34]

Auf folgende Entscheidungen wird näher hingewiesen:

1. Erkenntnis vom 24. Juni 2025, E 4624/2024
In dieser umfassenden Entscheidung betreffend die Neuorganisation der Finanzierung des Österreichischen Rundfunks (ORF) hat der VfGH u.a. ausgesprochen, dass § 13 und § 17 Abs. 7 und 8 ORF-Beitrags-Gesetz 2024,

BGBl I Nr. 112/2023, nicht gegen das Grundrecht auf Datenschutz verstoßen. Die ORF-Beitrags Service GmbH als Verantwortliche für die Festsetzung und Einhebung des ORF-Beitrags ist daher berechtigt, zur Erfassung aller Beitragsschuldner Daten aus dem Zentralen Melderegister (ZMR) und anderen Registern zu beziehen und zur Einbringung von ausständigen Beiträgen Daten an mit dem Inkasso beauftragte Dritte zu übermitteln, die hier von Gesetzes wegen als Auftragsverarbeiter tätig werden.

2. Beschluss vom 12. August 2025, DS 1/2025
In dieser Sache musste der VfGH nach Weiterleitung einer Datenschutzbeschwerde erstmals als „Datenschutzgericht erster und einziger Instanz" gemäß § 88b VfGG tätig werden. Der Beschwerdeführer behauptete mit näherer Begründung, durch die für ihn als Rechtsanwalt verpflichtende Verwendung des Web-ERV u.a. durch den VfGH in seinen durch Art. 5 und Art. 25 DSGVO garantierten (Datenschutz-)Rechten verletzt zu werden. Nach ausführlichen Erwägungen zur Frage, warum

30 Laut einer Suche nach Volltexten mit dem Norm-Suchbegriff „DSGVO oder DSG" im Rechtsinformationssystem des Bundes - RIS; Stand: 30. Jänner 2026.
31 vgl. neben dem unten angeführten etwa die Erkenntnisse vom 7. Oktober 2025, G 26/2025, in dem die Verfassungswidrigkeit einer bereits außer Kraft getretenen Bestimmung des BilDokG 2020 festgestellt wurde, und vom 10. Dezember 2025, E 2189/2025, betreffend Datenverarbeitung für Zwecke des WiEReG.
32 Veröffentlichung von Spenderdaten, vgl. dazu DSB Bescheid vom 4. Juli 2024, GZ: 2024-0.199.724.
33 Beschluss vom 11. September 2025, G 48/2025.
34 Beschluss vom 9. Dezember 2025, E 335/2025.

der Web-ERV als Datenverarbeitung für Zwecke der justiziellen Tätigkeit des VfGH nicht in den Zuständigkeitsbereich der DSB fällt, wies der VfGH die Beschwerde in der Sache ab. Es sei für den VfGH nicht erkennbar, inwiefern die vom Beschwerdeführer behaupteten technischen Schwierigkeiten für einen Rechtsanwalt bei der Verwendung des Web-ERV (z.B. behauptetermaßen falsche Sendebestätigungen bei Eingaben, keine Möglichkeiten von Eingabekorrekturen und ähnliches) einen Verstoß gegen Art. 5 oder Art. 25 DSGVO begründen können.

3. Erkenntnis vom 11. September 2025, E 1734/2025
Durch diese Entscheidung wurde das Erkenntnis des BVwG vom 2. Mai 2025, W137 2301309-1, das den Bescheid der DSB vom 5. September 2024, GZ: 2024-0.326.041 (Verfahrenszahl: D124.2577/23), bestätigt hatte, wegen Verletzung des Gleichheitssatzes laut Art. 7 B-VG sowie Art. 2 StGG und des Rechts auf Universitätsautonomie gemäß Art. 81c Abs. 1 B-VG aufgehoben. In einem Beschwerdeverfahren wegen heimlicher Tonaufnahmen von Universitätssitzungen ist in weiterer Folge näher zu prüfen, ob eine im Rahmen der autonomen Selbstverwaltung beschlossene Richtlinie einer Universität als Verordnung gilt und damit gemäß Art. 6 Abs. 1 lit. e DSGVO als Grundlage für solche Eingriffe herangezogen werden kann.

4. Erkenntnis vom 7. Oktober 2025, G 62/2025[35]
In diesem von einem Journalisten angestrengten Verfahren betreffend den Zugang zu Daten einer Gesellschaft im WiEReG leitete der VfGH amtswegig ein Gesetzesprüfungsverfahren betreffend § 10 f WiEReG ein. In seinem Erkenntnis kam der VfGH zu dem Schluss, dass § 10 Abs. 1 Z 1 WiEReG idF BGBl. I Nr. 97/2023 verfassungswidrig war, soweit damit Medien („Public Watchdogs"; Personen mit berechtigtem Interesse) der Zugang zu bestimmten Angaben im Wirtschaftliche-Eigentümer-Register verwehrt blieb. Die Interessenabwägung zwischen den Grundrechten nach Art. 10 EMRK (Informationsfreiheit) und § 1 DSG iVm Art. 8 EMRK (Datenschutz und Privatsphäre) ergab ein Überwiegen des ersteren. Da durch BGBl. I Nr. 151/2024 eine Novellierung der angewendeten, verfassungswidrigen Bestimmung erfolgte, konnte sich der VfGH auf die Feststellung der Rechtswidrigkeit beschränken.

5.2 Oberster Gerichtshof - OGH

1. Urteil vom 17. Jänner 2025, 6 ObA 2/23x
In einem Rechtsstreit zwischen einem Betriebsrat und der Betreibergesellschaft eines Essens-Zustelldienstes hielt der OGH, trotz Rückverweisung der Sache an das Erstgericht, fest, dass einem Betriebsrat gestützt auf die §§ 72 und 89 ArbVG ein Recht auf Kommunikation mit der Belegschaft zukommt. Die im Klagsweg begehrte Übermittlung der dem Arbeitgeber bekannten E-Mail-Adressen der Arbeitnehmer an den Betriebsrat ist in einer solchen Fallkonstellation daher datenschutzrechtlich gemäß Art 6 Abs 1 lit f DSGVO zulässig. Im Hinblick auf die vielfältigen Sanktionen im Fall der Verletzung der Verschwiegenheitspflicht durch ein Betriebsratsmitglied ist jedenfalls davon auszugehen, dass der Gesetzgeber angemessene Garantien für die Wahrung des Datenschutzes auch durch den Betriebsrat geschaffen hat.

2. Beschluss vom 3. Juli 2025, 6 Ob 62/25y
In dieser Sache hat der OGH entschieden, dass ein auf Art. 79 DSGVO und auf das Datenschutzrecht gestütztes zivilgerichtliches Vorgehen gegen die ORF-Beitrags Service GmbH (Klage auf Unterlassung der Verarbeitung von Daten des Klägers) nicht möglich ist, da die Beklagte bei der Einhebung

35 Siehe hierzu ausführlicher auch Newsletter 03/2025.

des ORF-Beitrags hoheitlich tätig wird. Art. 79 DSGVO ermöglicht zwar einen doppelgleisigen Rechtsschutz parallel zur Datenschutzbeschwerde gemäß Art. 77 DSGVO, erweitert aber nicht die Zuständigkeit der Zivilgerichte auf die Prüfung der Rechtmäßigkeit hoheitlichen Verwaltungshandelns, insbesondere da § 12 Abs 3 ORF-BeitragsG vorsieht, dass gegen Bescheide der Beklagten der Rechtsschutzweg einer Beschwerde an das BVwG eröffnet ist. Insofern liegt laut OGH kein bürgerlich-rechtlicher Anspruch gemäß § 1 JN vor.

3. Urteil vom 3. Juli 2025, 6 Ob 113/24x
In dieser Entscheidung wies der OGH eine Schadenersatzklage wegen verschiedener bereits gelöschter Marketingklassifikationen durch ein Direktmarketingunternehmen (Beklagte) endgültig ab. Aus einer Rechtsverletzung resultierende Gefühlsbeeinträchtigungen wie Ängste, Stress oder Leidenszustände aufgrund einer erfolgten oder auch nur drohenden Bloßstellung, Diskriminierung oder Ähnlichem können als immaterielle Schäden zu einem Schadenersatzanspruch nach Art 82 DSGVO führen. Eine besonders schwerwiegende Beeinträchtigung der Gefühlswelt ist nicht zu fordern. Das vom Kläger geltend gemachte Gefühl, durch Marketingklassifikationen in seiner Rechtssphäre in Form eines „abgestuften Grades des Ärgernisses" beeinträchtigt zu sein, reicht jedoch nicht aus, um einen ideellen Schaden auf Grundlage der Rechtsprechung des EuGH nachzuweisen.

4. Beschluss vom 13. August 2025, 6 Ob 15/25m
Mit diesem Beschluss hat der OGH in einem von einer Konsumentenschutzorganisation - mittels auf § 28a Abs 1 KSchG gestützte Unterlassungsklage - angestrengten Verfahren dem EuGH mehrere Fragen zur Auslegung von Art. 22 DSGVO betreffend die Verarbeitung von Scoring- und Profilingdaten durch ein Versandhandelsunternehmen vorgelegt (). Die Rechtssache ist beim EuGH zu C-568/25 anhängig.

5.3 Verwaltungsgerichtshof - VwGH

Der VwGH hat im Berichtsjahr[36] 2025 **57** veröffentlichte **Entscheidungen** in Rechtssachen getroffen, die vor der DSB ihren Ausgang genommen haben. In **42 Fällen**[37] ist in Erkenntnissen und Beschlüssen die DSGVO zur Anwendung gekommen. Aufgrund dieser Zahl an Entscheidungen musste hier eine enge Auswahl ohne Anspruch auf Vollständigkeit getroffen werden.

1. Erkenntnis vom 29. Jänner 2025, Ra 2023/04/0002[38]
Der VwGH hat sich in dieser Entscheidung sowie in weiteren, darauf aufbauenden Entscheidungen intensiv mit dem Ablehnungsrecht gemäß Art. 57 Abs. 4 DSGVO infolge des Urteils des EuGH vom 9. Jänner 2025, C-416/23 (siehe weiter unten) auseinandergesetzt. Die Ablehnung der Behandlung einer Beschwerde gemäß Art. 57 Abs. 4 DSGVO aus Gründen der Exzessivität setzt eine von der DSB nachzuweisende Missbrauchsabsicht der beschwerdeführenden Partei voraus. Von einer Missbrauchsabsicht ist insbesondere dann auszugehen, wenn die Erhebung von Datenschutzbeschwerden erfolgt, ohne dass dies objektiv erforderlich ist, um die der beschwerdeführenden Partei aus der DSGVO zukommenden Rechte zu schützen, sondern dies einem anderen Zweck dient, die beschwerdeführende Partei die Beschwerden etwa zur Erzielung eines nicht durch die

36 Laut einer Suche nach Volltexten mit der Wortfolge „belangte Behörde vor dem Verwaltungsgericht: Datenschutzbehörde" im Rechtsinformationssystem des Bundes - RIS; Stand: 30. Jänner 2026.
37 Laut einer Suche nach Volltexten mit dem Norm-Suchbegriff „32016R0679 Datenschutz-GrundV" laut VwGH-Normenliste im RIS; Stand: 30. Jänner 2026.
38 Siehe ausführlicher auch Newsletter 02/2025.

datenschutzrechtlichen Bestimmungen geschützten Zwecks erhebt (etwa Publicity, Feindseligkeit, Sensationslust). Das Vorliegen eines solchen Zwecks (= das Vorliegen von Missbrauchsabsicht) ist von der DSB und vom BVwG anhand aller relevanten Umstände jedes Einzelfalls zu beurteilen. Ein Indiz für Missbrauchsabsicht ist es bspw., wenn mit den Datenschutzbeschwerden die Verletzung des Auskunftsrechts nach Art. 15 DSGVO gegen eine Vielzahl von Verantwortlichen, die auf Auskunftsersuchen der beschwerdeführenden Partei keine Antwort gaben oder es ablehnten, dem Ersuchen zu entsprechen, geltend gemacht wird, die beschwerdeführende Partei jedoch zu den Verantwortlichen keinen Bezug hat, keine Anhaltspunkte für die Verarbeitung personenbezogener Daten der beschwerdeführenden Partei durch die Verantwortlichen bestehen oder der Kontakt zu den Verantwortlichen aus der Motivation heraus hergestellt wird, in der Folge datenschutzrechtliche Beschwerden einbringen zu können. Die Aufsichtsbehörde kann grundsätzlich wählen kann, ob sie eine angemessene Gebühr vorschreibt die Beschwerde ablehnt. Die Eignung der Gebühreneinhebung wird aber etwa dann zu verneinen sein, wenn die Vollstreckbarkeit der Gebührenvorschreibung auf Grund der finanziellen Lage der beschwerdeführenden Partei zweifelhaft ist oder angesichts der Annahme, dass die Rechtsschutzmöglichkeiten gegen einen Gebührenbescheid von der beschwerdeführenden Partei ebenfalls ausgenützt werden, um die Behörden lahmzulegen. Ebenso erweist sich die Gebühreneinhebung als ungeeignet, wenn trotz Gebührenvorschreibung für exzessive Datenschutzbeschwerden die beschwerdeführende Partei von der Einbringung solcher Beschwerden nicht Abstand nimmt. Das Vorliegen einer offenkundigen Unbegründetheit ist aus objektiver Sicht zu beurteilen. Eine Datenschutzbeschwerde ist dann offenkundig unbegründet, wenn bei vernünftiger Betrachtung des Vorbringens keinerlei Erfolgschance für den Einschreiter besteht.

2. Erkenntnis vom 30. April 2025, Ro 2021/04/0024[39]

Der VwGH hat mit dieser Entscheidung einen - vom BVwG zur Gänze bestätigten - Strafbescheid dem Grunde nach bestätigt. Der Revision wurde aber teilweise Folge gegeben, weil zum Zeitpunkt der Entscheidung des VwGH ein zusätzlicher Milderungsgrund bei der Strafbemessung berücksichtigt werden musste, nämlich die lange Verfahrensdauer von 5 Jahren. Der VwGH hat diesbezüglich in der Sache selbst entschieden und die Strafhöhe von ursprünglich EUR 3.000,- auf EUR 1.500,- reduziert. Der Beschuldigte hatte eine Videoüberwachungsanlage installiert, die neben seinem Objekt auch einen unmittelbar angrenzenden Gehsteig und öffentlichen Parkplatz erfasste. Es fehlte zudem jede Kennzeichnung der Überwachung und die Daten wurden 18 Tage gespeichert. Der VwGH sah keinen der behaupteten Verfahrensmängel als gegeben und bestätigte, dass eine Gesamtstrafe gemäß Art. 83 Abs. 3 DSGVO für alle festgestellten Verstöße im Zusammenhang mit der Videoüberwachungsanlage zu verhängen war. Spezielle Regelung in der DSGVO gehen entgegenstehenden nationale Bestimmungen des VStG vor. Dabei bestätigte der VwGH jedoch auch, dass Sanktionen nach Art. 83 DSGVO als eine „Verwaltungsstrafe“ zu werten sind, weshalb von der DSB die Bestimmungen des VStG grundsätzlich angewendet werden müssen.

3. Beschluss vom 8. Oktober 2025, Ra 2023/04/0117

Das betreffende Beschwerdeverfahren nahm seinen Ausgang bei der Verarbeitung von Daten des Zentralen Impfregisters für den Zweck der Versendung von Impferinnerungsschreiben während der COVID-19-Pandemie. Die DSB und das BVwG hatten diese Datenverarbeitung für rechtmäßig befunden. Der VwGH hat dies nun besätigt und eine außerordentliche Revision zurückgewiesen. Auf Basis der ausdrücklichen Bestimmung des § 750 Abs. 2 ASVG war der Dachverband der Sozialversicherungsträger ermächtigt, zum Zweck der Ermittlungen der gemäß Abs. 1 und Abs. 1a leg. cit. in Betracht kommenden Personen die im znetralen Impfregister (§24c GTelG 2012) gespeicherten Daten zu den COVID-19-Impfungen einmalig mit eigenen DAten zu verknüpfen bzw. abzugleichen, wobei die Adressermittlung aus dem beim Dachverband der Sozialversicherungs-

39 Siehe hierzu ausführlicher auch Newsletter 02/2025.

träger selbst eingerichteten Patientenindex zum Zweck der Übermittlung der gemäß §750 Abs. 1a ASVG ausdrücklich angeordneten Information ohne Zweifel mitumfasst sein musste. Weiters hielt der VwGH fest, dass nicht jede Verletzung der Informationspflicht gemäß Art. 14 DSGVO per se zur Unrechtmäßigkeit einer Datenverarbeitung und damit zu einer Verletzung im Recht auf Geheimhaltung führt.

4. Erkenntnis vom 17. Dezember 2025, Ro 2023/04/0029
In dieser Entscheidung wurde nach ordentlicher Amtsrevision der DSB ein Erkenntnis des BVwG aufgehoben. Streitgegenstand war die Auslegung von Art. 4 Z 4 und Art. 15 Abs.1 lit. h DSGVO im Zuge eines Rechtsstreits betreffend di Auskunfterteilung über Datenverarbeitung für Zwecke der Zuschreibung von Marketingklassifikationen durch ein Direktmarketingunternhemen. Der VwGH bekräftigte dabei, entgegen dem Vorbringen der DSB, seine bestehende Rechtsprechung, wonach das Auskunftsrecht des Art. 15 Abs. 1 lit. h DSGVO das Bestehen einer automatisierten Entscheidungsfindung im Sinn des Art. 22 DSGVO voraussetzt. Dafür bedarf es als einer von mehreren Voraussetzungen einer rechtlichen Wirkung der Entscheidung gegenüber der betroffenen Person oder einer erheblichen Beeinträchtigung in ähnlicher Weise. Dies ist auch dann gegeben, wenn das Ergebnis der automatisierten Entscheidungsfindung eine maßgebliche Rolle für eine gegenüber der betroffenen Person getroffene Entschidung spielt. Um das Bestehen eines Auskunftsanspruchs nach Art. 15 Abs. 1 lit. h DSGVO beurteilen zu können, bedarf es entsprechender Feststellungen zu den dargelegten Voraussetzungen. Da das BVwG aber entsprechende Sachverhaltsfeststellungen unterlassen hatte (sogenannte sekundäre Feststellungsmängel), wurde das Erkenntnis wegen Rechtswidrigkeit des Inhalts aufgehoben.

5. Erkenntnis vom 17. Dezember 2025, Ra 2024/04/0310
Gegenstand dieser Entscheidung war die Datenschutzbeschwerde eines nicht-richtlichen Beamten des BVwG gegen den Präsidenten dieses Gerichts wegen Datenverarbeitung für Zwecke einer in Ausübung der Dienstaufsicht vorgenommenen Nachschau im unversperrten Büro des Beschwerdeführers, bei der auch Fotos angefertigt wurden. Die DSB und das BVwG hatten die Beschwerde abgewiesen, letzteres auch die ordentliche Revision nicht zugelassen. Der VwGH erachtete die erhobene außerordntliche Revision im Hinblick auf die aufgeworfene Frage, ob Datenverarbeitung für Maßnahmen der Dienstaufsicht überhaupt in die Zuständigkeit der DSB (oder hier unter justizielle Tätigkeit gemäß Art. 55 Abs. 3 DSGVO) fällt, für zulässig, jedoch in der Sache für unbegründet. Maßnahmen der Dienstaufsicht gemäß § 3 Abs. 1 BVwGG erfolgen im Zuge der monokratischen Justizverwaltung und sind daher nicht als solche eines Gerichts im Sinne des Art. 55 Abs. 3 DSGVO anzusehen. Dieser Auslegung steht auch die vorliegende Rechtsprechung des EuGH (weites Verständnis des Begriffs der "justiziellen Tätigkeit" in Art. 55 Abs. 3 DSGVO, insbeosndere das Urteil vom 24. März 2022, C-245/20) nicht entgegen. Da auch keine relevanten Verfahrensmängel aufgezeigt wurden, wurde die Beschwerde abgewiesen.

5.4 Europäischer Gerichtshof für Menschenrechte - EGMR

Im Berichtszeitraum war wiederum eine Reihe von Entscheidungen in Beschwerdeverfahren betreffend **Art. 8 (und 10) EMRK** zu verzeichnen[40], die vor dem besonderen Hintergrund des Ausscheidens Russlands aus dem Anwendungsbereich der EMRK zu sehen sind.[41]

40 z.B. Urteile vom 4. Februar 2025, Appl. Nr. 33421/16 u.a., und vom 27 Mai 2025, Appl. Nr. 39056/22 u.a.
41 Die Russische Föderation ist seit dem 16. September 2022 keine Vertragspartei der Europäischen Menschenrechtskonvention mehr, der EGMR kann nur mehr Sachverhalte prüfen, die sich bis dahin ereignet haben.

Auf folgende weitere Entscheidungen wird hingewiesen:

1. Urteil vom 4. Dezember 2025, Appl. Nr. 36325/22
Diese Entscheidung ist insofern bemerkenswert, als sie die übliche datenschutzrechtliche Perspektive umkehrt. Eine leitende Angestellte eines spanischen Unternehmens hatte zunächst erfolgreich ein arbeitsgerichtliches Verfahren gegen ihren Arbeitgeber geführt, dem sie durch den ihr beruflich eingeräumten Zugriff auf sämtliche Gehaltsdaten im Unternehmen Diskriminierung aufgrund ihres Geschlechts bei der Gehaltshöhe nachweisen konnte. In weiterer Folge wurde sie u.a. wegen der mit der Beschaffung der Vergleichsdaten verbundenen Verletzung des Datenschutzes entlassen. Eine Anfechtung dieser Entscheidung vor den Gerichten bliebt erfolglos. Der EGMR entschied, dass eine Verletzung von Art. 14 EMRK (ungerechtfertigte Diskriminierung) erfolgte, da die Gerichte im zweiten Rechtsstreit dem Zweck der Offenlegung der Daten Dritter, nämlich die Beseitigung einer ungerechtfertigten Diskriminierung, zu wenig und deren Datenschutzrechten als Entlassungsgrund zu viel Gewicht zugemessen hatten.

2. Urteil vom 18. Dezember 2025, Appl. Nr. 37514/20 u.a.
In dieser Sache entschied der EGMR, dass die tschechischen Polizei- und Justizbehörden mehrere Strafverteidiger in ihrem Recht auf Schutz der beruflichen Privatsphäre gemäß Art. 8 EMRK verletzt haben, indem sie sich weigerten, Daten, die sie von beschlagnahmten elektronischen Geräten eines Mandanten der Beschwerdeführer gewonnen hatten, aus den Ermittlungsakten zu löschen, soweit sie vertrauliche Korrespondenz zwischen dem Beschuldigten und seinen Verteidigern betrafen. Mangels einer jedenfalls im Zeitraum 2016 bis 2019 (endgültige Abweisung einer Beschwerde durch das tschechische Verfassungsgericht) anwendbaren Rechtsschutzbestimmung für solche Fälle wurde auch das Recht auf eine wirksame Beschwerde gemäß Art. 13 EMRK verletzt.

5.5 Gerichtshof der Europäischen Union - EuGH

Der EuGH hat im Berichtszeitraum **18 Vorabentscheidungsverfahren** mit dem Gegenstand „Schutz personenbezogener Daten“ abgeschlossen.[42]

Auf folgende Entscheidungen wird hingewiesen:

1. Urteil vom 9. Jänner 2025, C-394/23
Obwohl der Gegenstand dieser Sache vordergründig das „richtige Gendern“ war, oder in den Worten des EuGH: „die Verarbeitung personenbezogener Daten hinsichtlich der Anrede der Kunden eines Transportunternehmens, die darauf abzielt, die geschäftliche Kommunikation aufgrund ihrer Geschlechtsidentität zu personalisieren“, wurde hier darüber hinaus über Fragen von Erforderlichkeit einer Datenverarbeitung für Zwecke einer Vertragserfüllung und Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO entschieden. Ein Unternehmen der französischen Staatsbahn SNCF hatte beim Online-Fahrscheinkauf die binäre Angabe des Geschlechts [Mann oder Frau] als Pflichtfeld definiert. Der EuGH verwies auf seine Vorjudikatur, dabei insbesondere auf das Urteil vom 4. Juli 2023, C-252/21, und kam zu dem Schluss, dass eine Personalisierung der geschäftlichen Kommunikation, die auf einer anhand der Anrede angenommenen Geschlechtsidentität beruht, weder objektiv unerlässlich noch wesentlich ist, um die ordnungsgemäße Erfüllung des betreffenden Vertrags zu ermöglichen.

42 Einschließlich Streichungen nach Zurückziehung des Vorabentscheidungsersuchens.

2. Urteil vom 9. Jänner 2025, C-416/23
Diese Rechtssache nahm ihren Ausgangspunkt bei der DSB, die die Behandlung einer Beschwerde wegen Verletzung des Auskunftsrechts gemäß Art. 57 Abs. 4 DSGVO abgelehnt hatte, weil der Beschwerdeführer innerhalb eines Zeitraums von ca. 20 Monaten 77 ähnliche Beschwerden gegen verschiedene Verantwortliche eingebracht hatte. Das BVwG hob diesen Bescheid mit der tragenden Begründung auf, das rechtsmissbräuchliche Handeln des Beschwerdeführers sei damit nicht erwiesen. Der im Wege einer Amtsrevision angerufene VwGH legte dem EuGH verschiedene Fragen zur Auslegung von Art. 57 Abs. 4 DSGVO vor. Der EuGH hielt zunächst fest, dass unter „Anfragen" an eine Datenschutz-Aufsichtsbehörde jedenfalls auch Beschwerden gemäß Art. 77 DSGVO zu verstehen sind. Weiters können solche „Anfragen" nicht allein aufgrund ihrer Zahl während eines bestimmten Zeitraums als „exzessiv" im Sinne dieser Bestimmung eingestuft werden, da die Ausübung der in dieser Bestimmung vorgesehenen Befugnis voraussetzt, dass die Aufsichtsbehörde das Vorliegen einer Missbrauchsabsicht der anfragenden Person nachweist. Die Aufsichtsbehörde kann bei exzessiven Anfragen durch eine mit Gründen versehene Entscheidung wählen, ob sie eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangt oder sich weigert, aufgrund der Anfrage tätig zu werden, wobei sie alle relevanten Umstände berücksichtigen und sich vergewissern muss, dass die gewählte Option geeignet, erforderlich und verhältnismäßig ist.

3. Urteil vom 13. Februar 2025, C-383/23
In dieser Entscheidung hat der EuGH klargestellt, dass der Begriff „Unternehmen" im Sinne des Art. 83 Abs. 4 bis 6 DSGVO dem Begriff „Unternehmen" im Sinne der Art. 101 und 102 AEUV entspricht, so dass der Höchstbetrag einer Geldbuße, die gegen einen Verantwortlichen für personenbezogene Daten, der ein Unternehmen ist oder einem Unternehmen angehört, wegen eines Verstoßes gegen die DSGVO verhängt wird, auf der Grundlage eines Prozentsatzes des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs des Unternehmens bestimmt wird. Der Begriff „Unternehmen" ist auch zu berücksichtigen, um die tatsächliche oder materielle Leistungsfähigkeit des Adressaten der Geldbuße zu beurteilen und so zu überprüfen, ob die Geldbuße sowohl wirksam und verhältnismäßig als auch abschreckend ist.

4. Urteil vom 27. Februar 2025, C-203/22
In dieser Sache, die ihren Ausgang in einem Verfahren vor dem Verwaltungsgericht Wien (VGW) betreffend die Vollstreckung eines Erkenntnisses des BVwG in einem Datenschutzbeschwerdeverfahren, hat der EuGH die Auslegung von Art. 15 Abs. 1 lit. h DSGVO präzisiert. Die Bestimmung ist dahingehend auszulegen, dass bei automatisierten Entscheidungsfindungen (einschließlich Profilings) im Sinne von Art. 22 Abs. 1 DSGVO die betroffene Person vom Verantwortlichen im Rahmen des Anspruchs auf Erteilung „aussagekräftiger Informationen über die involvierte Logik" verlangen kann, ihr anhand der maßgeblichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form die Verfahren und Grundsätze zu erläutern, die bei der automatisierten Verarbeitung ihrer personenbezogenen Daten zur Gewinnung eines bestimmten Ergebnisses - beispielsweise eines Bonitätsprofils - konkret angewandt wurden. Ein Verantwortlicher, der sich zur Abwehr eines Auskunftsanspruchs auf den Schutz von Geschäftsgeheimnissen beruft, muss diese angeblich geschützten Informationen der zuständigen Aufsichtsbehörde oder dem zuständigen Gericht übermitteln, die die einander gegenüberstehenden Rechte und Interessen abwägen müssen, um den Umfang des in Art. 15 DSGVO vorgesehenen Auskunftsrechts der betroffenen Person zu ermitteln.

5. Urteil vom 27. Februar 2025, C-638/23
In dieser verfahrensrechtlich bedeutenden Sache hat der EuGH aufgrund eines vom VwGH in einem Revisionsverfahren betreffend den Versand von „Impferinnerungsschreiben" gestellten Vorabentscheidungsersuchens entschieden, dass eine nationale Regelung, in der ein Hilfsapparat verschiedener Behörden ohne eigene Rechtspersönlichkeit (hier: das Amt der Tiroler Landesre-

gierung) zum für die Verarbeitung personenbezogener Daten Verantwortlichen bestimmt wurde, nicht gegen Art. 4 Z 7 DSGVO verstößt, sofern zum einen eine solche Stelle gemäß dieser nationalen Regelung die Pflichten zu erfüllen vermag, die ein Verantwortlicher gegenüber den betroffenen Personen im Bereich des Schutzes personenbezogener Daten hat, und zum anderen diese nationale Regelung explizit oder zumindest implizit den Umfang der Verarbeitung personenbezogener Daten vorgibt, für die diese Stelle verantwortlich ist.

6. Urteil vom 2. Dezember 2025, C-492/23

Dieses Verfahren, dem ein Vorabentscheidungsersuchen eines Gerichts aus Rumänien zugrunde lag, betraf die datenschutzrechtliche Verantwortlichkeit eines Unternehmens, das eine Online-Marktplatz betreibt. Auf dieser Plattform waren gefälschte Online-Inserate erschienen, die die Klägerin im Ausgangsverfahren, die gemäß Art. 82 DSGVO vom Unternehmen Schadenersatz verlangte, als Anbieterin sexueller Dienstleistungen erscheinen ließen. Der EuGH hat entschieden, dass der Betreiber eines Online-Marktplatzes als gemeinsamer Verantwortlicher gemäß Art. 26 DSGVO mit dem Inserenten haftet und vor der Veröffentlichung auch gemäß Art. 32 DSGVO mittels geeigneter technischer und organisatorischer Maßnahmen verpflichtet ist, Anzeigen, die sensible Daten im Sinne von Art. 9 Abs. 1 DSGVO enthalten, zu identifizieren, die Identität von Inserent und betroffener Person zu prüfen, und die Veröffentlichung gegebenenfalls zu verweigern, es sei denn, der Inserent kann nachweisen, dass die betroffene Person ausdrücklich in die Veröffentlichung der fraglichen Daten auf diesem Online-Marktplatz eingewilligt hat oder dass eine der anderen in Art. 9 Abs. 2 lit. b bis j DSGVO vorgesehenen Ausnahmen erfüllt ist.

6. Europäische Zusammenarbeit

6.1 Europäischer Datenschutzausschuss

Im EDSA wurde im Jahr 2025 eine der beiden Positionen des:der stellvertretenden Vorsitzenden neu besetzt, da die nationale Amtszeit einer der beiden stellvertretenden Vorsitzenden am 27. September 2025 endete. Nach zwei geheimen Wahlgängen wurde die Leiterin der slowenischen Aufsichtsbehörde, **Dr.in Jelena Virant Burnik**, für die nächsten fünf Jahre in das zweite Amt der stellvertretenden Vorsitzenden gewählt und folgt in dieser Funktion der Leiterin der zypriotischen Aufsichtsbehörde, **Irene Loizidou Nicolaidou**, nach. Der übrige Vorsitz im EDSA hat 2025 keine Änderung erfahren.

Die **Vollversammlung des EDSA** hat sich im Jahr 2025 insgesamt **12 Mal getroffen**, wobei **eine** außerordentliche Versammlung einberufen wurde. **4 Treffen fanden vor Ort** in Brüssel statt und **8 Treffen** wurden **per Videokonferenz** abgehalten.

Die im Rahmen der Plenarsitzungen besprochenen Themen und angenommenen Dokumente wurden in den Fachgruppen[43] des EDSA vorbereitet, die im Jahr 2025 regelmäßige Arbeitssitzungen sowohl vor Ort in Brüssel als auch per Videokonferenz abgehalten haben. Eine Auswahl dieser Dokumente wird im Folgenden näher dargelegt.

Der EDSA hat gemäß **Art. 64 DSGVO** im Jahr 2025 insgesamt **28 Stellungnahmen**[44] zu folgenden Themen abgegeben:

- **25** Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (Coface Group, Alfa Laval Group, 2 Mal Nokia Group, 2 Mal Worldline Group, Statkraft Group, Signify Group, ASML Group, Wilh. Wilhelmsen Group, Aramex Group, 2 Mal Shopify Group, 2 Mal Northern Trust Group, Mowi Group, Ferrero Group, Tessi Group, 2 Mal BOX Group, 2 Mal Ilumina Group, Arcadis Group, 2 Mal CSG Group); und

- **3** Stellungnahmen zu nationalen Zertifizierungskriterien (Frankreich, Österreich, Griechenland);

Gemäß **Artikel 70 DSGVO** wurden vom EDSA im Jahr 2025 insgesamt **5 Stellungnahmen** zu folgenden Themen abgegeben:

- zur Verlängerung der Adäquanzentscheidung der Europäischen Kommission über die Angemessenheit des Datenschutzniveaus im Vereinigten Königreich Großbritannien und Nordirland (Stellungnahme 06/2025);

- zur Adäquanzentscheidung der Europäischen Kommission über die Angemessenheit des Datenschutzniveaus der Europäischen Patentorganisation (Stellungnahme 07/2025);

43 Eine Übersicht der bestehenden Fachgruppen ist in englischer Sprache abrufbar unter https://www.edpb.europa.eu/about-edpb/who-we-are/edpb-plenaries-subgroups-and-taskforces_en.

44 Siehe hierzu https://www.edpb.europa.eu/our-work-tools/consistency-findings/opinions_de?f%5B0%5D=opinions_date%3A2025.

- 2 Mal zur Adäquanzentscheidung der Europäischen Kommission über die Angemessenheit des Datenschutzniveaus im Vereinigten Königreich Großbritannien und Nordirland (Stellungnahmen 26/2025 und 27/2025);

- zur Adäquanzentscheidung der Europäischen Kommission über die Angemessenheit des Datenschutzniveaus von Brasilien.

Ferner wurde im Jahr 2025 **1 gemeinsame Stellungnahme** des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten in folgender Angelegenheit erlassen:

- zum Vorschlag für eine Verordnung über Vereinfachungsmaßnahmen für KMUs, insbesondere im Hinblick auf die Aufzeichnungspflichten nach Artikel 30 Absatz 5 DSGVO (gemeinsame Stellungnahme 01/2025).

Der EDSA hat im Jahr 2025 zu folgenden Themen neue **Leitlinien**[45] verabschiedet:

- zur Pseudonymisierung (EDPB Guidelines 01/2025);

- zur Verarbeitung personenbezogener Daten mittels Blockchain-Technologien (EDPB Guidelines 02/2025);

- zum Zusammenspiel zwischen dem DSA und der DSGVO (EDPB Guidelines 03/2025).

Darüber hinaus wurden die **ersten gemeinsamen Leitlinien des Europäischen Datenschutzausschusses und der Europäischen Kommission** in folgender Angelegenheit beschlossen:

- zum Zusammenspiel zwischen dem DMA und der DSGVO.

Des Weiteren wurde folgende **endgültige Fassung einer Leitlinie** angenommen:

- zu Art. 48 DSGVO (EDPB Guidelines 02/2024, Version 2.1).

Schlussendlich wurden vom Europäischen Datenschutzausschuss im Jahr 2025 zu folgenden Themen neue **Empfehlungen** ausgesprochen:

- zum Welt-Anti-Doping-Kodex 2027 der WADA (Empfehlung 01/2025);

- zur rechtlichen Grundlage für die Pflicht zur Erstellung von Benutzerkonten auf E-Commerce-Websites (Empfehlung 02/2025).

Aufgrund der budgetären und personellen Lage (siehe **Kapitel 3.2.**) konnten seitens der DSB im Jahr 2025 **nicht mehr alle Fachgruppen des EDSA beschickt** werden. Die DSB hat ihre Ressourcen insbesondere auf jene Fachgruppen konzentriert, die besonders wichtig für das Tagesgeschäft der DSB sind. Als weitere Maßnahme wurden Dienstreisen zu Vor-Ort-Treffen der Fachgruppen in Brüssel eingeschränkt und erfolgten nur im unbedingt erforderlichen Ausmaß.

Nachdem in Österreich seit 1. Jänner 2025 mit dem PDK eine zweite Datenschutz-Aufsichtsbehörde eingerichtet wurde, ist gesetzlich vorgesehen, dass der **Leiter der DSB als gemeinsamer**

45 Siehe https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de?f%5B0%5D=opinions_date%3A2025.

Vertreter im EDSA und als zentrale Anlaufstelle fungiert.[46] Die DSB hat das PDK in Bezug auf den EDSA über alle Angelegenheiten zu informieren und einzubinden, wenn es davon betroffen sein könnte.[47] Die DSB und das PDK haben aus diesem Grund entsprechende Kommunikationskanäle eingerichtet, um einen Informationsaustausch sicherzustellen.

6.2 Europol

Das **Europäische Polizeiamt** 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 (EU) 2016/794**,[48] zuletzt geändert durch die **Verordnung (EU) 2022/991**,[49] 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.

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.

46 Vgl. § 35i DSG.
47 Vgl. § 35i DSG.
48 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0794, abgerufen am 18.02.2026.
49 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R0991, abgerufen am 18.02.2026.

6.3 Schengen - einschließlich Schengen Evaluierung Österreich sowie Visa Informationssystem und Entry Exit System

6.3.1 Allgemeines

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 eine gemeinsame Datenbank, die von nationalen Behörden wie Polizei und Grenzschutz eingegeben und in Echtzeit abgefragt werden können.

Die Rechtsgrundlagen für das SIS sind in **drei Verordnungen** der EU geregelt.[50]

Die DSB ist als Aufsichtsbehörde verpflichtet, regelmäßige „Audits" des nationalen Schengen-Systems durchzuführen.

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 EU sowie assoziierten Ländern ermöglicht.

Die Rechtsgrundlage für das VIS bildet die **VIS-Verordnung**[51].

Die DSB ist als Aufsichtsbehörde verpflichtet, regelmäßige „Audits" des nationalen VIS-Systems durchzuführen.

Beginnend mit 12. Oktober 2025 wurde das **Einreise-/Ausreisesystem** (kurz **„EES"**) an den Außengrenzen der EU in Betrieb genommen und wird schrittweise an den Grenzübergangsstellen bis zum 10. April 2026 vollständig umgesetzt. Das EES ist ein automatisiertes Grenzmanagementsystem für Kurzaufenthalte (bis zu 90 Tagen), das Drittstaatsangehörige, bei jedem Übertritt der Außengrenzen registriert. In Österreich betrifft dies Flughäfen und Flugplätze als Grenzübergangsstellen.

Die Rechtsgrundlage für die Verarbeitung personenbezogener Daten im EES ist in der – unmittelbar anwendbaren – **EES-Verordnung**[52] der EU geregelt.

Die DSB ist als Aufsichtsbehörde verpflichtet, regelmäßige „Audits" des nationalen EES-Systems durchzuführen.

---

50 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;

51 Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung).

52 Verordnung (EU) 2017/2226 des europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011

6.3.2 Beschwerden

Um die Rechte Betroffener sicherzustellen, hat die EU in sämtlichen der genannten Verordnungen Auskunfts- Berichtigungs- und Löschungsrechte (bei unrechtmäßiger Verarbeitung) festgelegt. Diese können im Streitfall vor den nationalen DSB geltend gemacht werden.

Die DSB beobachtete in diesem Zusammenhang im Jahr 2025 einen **sprunghaften Anstieg der Lösch-Beschwerden aus dem SIS**. Es sind alleine im letzten Jahr **468 neue Löschbeschwerden zum SIS**, insbesondere im Zusammenhang mit der Eintragung von Rückkehrentscheidungen (negative Asylbescheide) durch Österreich in das SIS bei der DSB eingegangen.

Die DSB hat zu diesen Lösch-Beschwerden **Informationen auf ihrer Webseite** veröffentlicht:

https://dsb.gv.at/aktuelles/information-der-datenschutzbehoerde-zu-loeschantraegen-von-sis-ausschreibungen

Die entwickelte Judikaturlinie der DSB (Abweisung der Lösch-Beschwerde, soweit nicht ein anderer Mitgliedsstaat einen Aufenthaltstitel zu erteilen beabsichtigt und dies im Rahmen einer Vorabkonsultation gemäß **Art. 9 der SIS-Verordnung** Rückkehr dem ausschreibenden Staat (hier Österreich) mitteilt), wurde bereits in einigen Entscheidungen durch das BVwG bestätigt.

6.3.3 Schengen Evaluierung Österreich 2025

Die **Europäische Kommission prüft** in regelmäßigen Abständen (bislang alle 5 Jahre) gemeinsam mit nationalen Experten der Mitgliedsstaaten die **Umsetzung der SIS – Verordnungen, der VIS-Verordnung und in Zukunft auch der EES-Verordnung in den einzelnen Mitgliedstaaten**.

Eine derartige Schengen–Evaluierung fand für den Bereich „Datenschutz“ von **19. Mai bis 23. Mai 2025** mit zahlreichen On-site-visits des Evaluierungs-Teams bei der DSB, Polizeidienststellen und im Außenministerium (VIS) statt. Die DSB war durchgehend mit Mitarbeitern – wie bei Schengen – Evaluierungen im Bereich Datenschutz üblich - präsent. Zeitgleich bzw. kurz davor und kurz danach fanden „polizeiliche Schengen-Evaluierungen“ im Bereich „Border Management“, „Return“, „Police Co-operation“ und „SIS“ statt. Eine Veröffentlichung des Abschlussberichtes zur Schengen-Evaluierung 2025 steht zu Redaktionsschluss des Tätigkeitsberichtes unmittelbar bevor.

Darüber hinaus nahm eine Mitarbeiterin im Jahr 2025 an der Schengen Evaluierung in Slowenien teil.

6.4 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**.[53]

53 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:01997R0515-20210101, abgerufen am 18.02.2026.

Zur Gewährleistung eines angemessenen Datenschutzes wurde neben dem Ausschuss **(„Joint Supervisory Authority of Customs“)** eine Koordinierende Aufsichtsbehörde **(CIS Supervision Coordination Group)** eingerichtet, welche aus Vertreter:innen der nationalen 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 von beim EDSA eingerichteten Komitee **(Coordinated Supervision Committee)** übernommen werden.

6.5 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**.[54]

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. 603/2013** 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.

Im Jahr 2025 wurde **ein Prüfverfahren im Bereich Eurodac** abgeschlossen.

6.6 Hochrangige Gruppe nach Artikel 40 des Gesetzes über digitale Märkte

Die **Verordnung (EU) 2022/1925** über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der **Richtlinien (EU) 2019/1937 und (EU) 2020/1828** (Gesetz über digitale Märkte) – besser bekannt als **Digital Markets Act (DMA)** – sieht in **Art. 40** die sogenannte **„Hochrangige Gruppe“ („High Level Group“)** vor.

Diese besteht aus Vertreter:innen

- des Gremiums europäischer Regulierungsstellen für elektronische Kommunikation;
- des Europäischen Datenschutzbeauftragten und Europäischen Datenschutzausschusses;

54 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013R0603, abgerufen am 18.02.2026.

- des Europäischen Wettbewerbsnetzes;
- des Netzwerks für die Zusammenarbeit im Verbraucherschutz;
- der Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste.

Der Leiter der DSB wurde vom EDSA in der Plenarsitzung vom 5.5.2025 als eines von vier vom EDSA zu entsendenden Mitgliedern gewählt. **Die anderen gewählten Mitglieder sind: Dale Sunderland (Irland); Mirosław Wróblewski (Polen), Jekaterina Macuka (Lettland) und Bruno Lasserre (FR)**.

Die hochrangige Gruppe dient der Beratung der Europäischen Kommission.

Die 5. Sitzung fand am 12. Dezember 2025 in Brüssel statt. Dabei wurde insbesondere das Positionspapier zu künstlicher Intelligenz angenommen.[55]

55 Siehe https://digital-markets-act.ec.europa.eu/fifth-meeting-digital-markets-act-high-level-group-2025-12-12_en, abgerufen am 18.02.2026.

7. Internationale Beziehungen

Die Aufsichtsbehörden der Mitgliedstaaten der EU und des Europarates treffen sich einmal im Jahr zu einem gegenseitigen Austausch im Rahmen der **„Spring Conference“**[56]. In diesem Forum werden insbesondere Kooperationsmöglichkeiten zwischen den Aufsichtsbehörden sowie Themen von gemeinsamem Interesse besprochen.

Die **Spring Conference 2025** wurde vom 6. bis 9. Mai 2025 von der georgischen Aufsichtsbehörde in Batumi ausgerichtet, wobei am 7. und 8. Mai 2025 die geschlossene und am 9. Mai 2025 die offene Sitzung stattfanden. Die DSB war mit ihrem Leiter sowie dem Abteilungsleiter der internationalen Abteilung vertreten.

Die geschlossene Sitzung wurde für einen Austausch zum Zusammenspiel der DSGVO und der KI-VO, dem Schutz Minderjähriger in einer KI-getriebenen Umgebung, der Verarbeitung von Gesundheitsdaten, der Rolle und den Aufgaben von Datenschutzbeauftragten, der Behandlung von Masseverfahren sowie der grenzüberschreitenden Zusammenarbeit zwischen Aufsichtsbehörden genutzt. Die offene Sitzung war gänzlich den Herausforderungen durch KI gewidmet.

Im Rahmen der Spring Conference 2025 wurden folgende Resolutionen[57] angenommen:

- Resolution über die Akkreditierung der kosovarischen Aufsichtsbehörde als Mitglied mit „other specific status“;
- Resolution über die Akkreditierung der andalusischen Aufsichtsbehörde als Mitglied mit dem Status „European sub-national data protection authority“;
- Resolution zum Aktionsplan für weitere Kooperationsaktivitäten

Die Spring Conference 2026 wird von der türkischen Aufsichtsbehörde veranstaltet.

Daneben bildet die **Konferenz der Internationalen Datenschutzversammlung (Global Privacy Assembly)**[58] seit mehr als vier Jahrzehnten ein globales Forum für Datenschutz-Aufsichtsbehörden aus aller Welt.

Im Jahr 2025 wurde die GPA von der südkoreanischen Aufsichtsbehörde vom 15. bis 19. September 2025 in Seoul abgehalten, wobei vom 15. bis 17. September 2025 die offene und vom 18. bis 19. September 2025 die geschlossene Sitzung stattfanden. Die DSB hat von einer Teilnahme an der GPA im Jahr 2025 aus Kostengründen abgesehen.

In der offenen Sitzung wurden insbesondere Fragen der Verarbeitung personenbezogener Daten iZm KI, der Schutz von Minderjährigen sowie Rechtsschutzmöglichkeiten von Betroffenen diskutiert. Am Ende der offenen Sitzung wurde zum fünften Mal der "Giovanni Buttarelli Award" verliehen, der 2025 an die Leiterin der argentinischen Aufsichtsbehörde und Komiteevorsitzende der Datenschutzkonvention 108, **Beatriz de Anchorena**, ging.[59]

---

56 Siehe https://www.dpaspringconference.org/about-us/.
57 Siehe https://www.dpaspringconference.org/resolution/.
58 Siehe https://globalprivacyassembly.com/.
59 Siehe https://www.coe.int/en/web/data-protection/-/convention-108-chair-receives-giovanni-buttarelli-award.

In der geschlossenen Sitzung stellten die Arbeitsgruppen der GPA sowie ihre Beobachter:innen und Partnerorganisationen ihre Tätigkeitsberichte vor. Darüber hinaus wurden folgende Resolutionen[60] angenommen:

- Resolution zur Erhebung, Nutzung und Weitergabe von personenbezogenen Daten zum Vortraining, Training und zur Feinabstimmung von KI-Modellen;
- Resolution zur sinnvollen menschlichen Kontrolle von Entscheidungen im Zusammenhang mit KI-Systemen;
- Resolution zu digitaler Bildung, Datenschutz und personenbezogenen Daten für eine verantwortungsvolle und inklusive digitale Bürgerschaft

Die GPA wird im Jahr 2026 von der Aufsichtsbehörde von Dubai ausgerichtet.

7.1 Bilaterale Kooperationen und Treffen der Datenschutz-Aufsichtsbehörden

Neben der Zusammenarbeit im Rahmen des EDSA legt die DSB großen Wert auf bilaterale Kooperationen mit anderen Aufsichtsbehörden. Im Fokus der Bemühungen der DSB stehen vorranging, aber nicht ausschließlich, Aufsichtsbehörden in den Nachbarländern der Republik Österreich, die vergleichbare Größen und Strukturen aufweisen und vor ähnlichen Herausforderungen stehen.

Zu Beginn des Jahres 2025 nutzte die DSB ihren traditionellen Neujahrsempfang am 14. Jänner 2025 für eine Einladung der **kroatischen Aufsichtsbehörde**, deren Leiter **Zdravko Vukić** den Vizevorsitz im EDSA innehat. Der Besuch der kroatischen Kolleg:innen in Wien wurde in weiterer Folge für ein Arbeitsgespräch am 15. Jänner 2025 genutzt, in welchem Angelegenheiten von gemeinsamem Interesse besprochen und die gegenseitige Kooperation weiter vertieft wurde.

Vom 24. bis 28 Februar 2025 erfolgte ein Arbeitsbesuch bei der **irischen Aufsichtsbehörde** in Dublin, um die dortigen Abläufe vor Ort kennenzulernen und Aspekte der täglichen Zusammenarbeit zu besprechen. Der irischen Aufsichtsbehörde kommt im Gefüge der EU-Aufsichtsbehörden eine wesentliche Rolle zu, da viele global agierende Verantwortliche ihre EU-Hauptniederlassung in Irland haben. Da bei der DSB regelmäßig Beschwerden gegen Verantwortliche mit Hauptsitz in Irland eingebracht werden, ist eine gut vernetzte Kooperation wichtig.

Die DSB folgte vom 24. bis 26. März 2025 der Einladung des Leiters der **tschechischen Aufsichtsbehörde**, **Mgr. Jiří Kaucký**, nach Prag. Im Rahmen der Arbeitsgespräche wurden vor allem die nationalen Zuständigkeiten abseits der DSGVO und verschiedene Aspekte der Verfahrensführung sowie der Entscheidungspraxis besprochen. Von besonderer Relevanz waren für die DSB ferner die jahrelangen praktischen Erfahrungen der tschechischen Aufsichtsbehörde im Bereich der Informationsfreiheit und es gab zu diesem Thema vom 23. bis 25. Juli 2025 einen weiteren Arbeitsbesuch der DSB in Prag.

60 Siehe https://globalprivacyassembly.com/document-archive/adopted-resolutions/.

Am 16. Juli 2025 konnte die DSB in Wien eine Delegation der **slowakischen Aufsichtsbehörde** unter Führung ihrer neue Leiterin **Zuzana Valková** begrüßen. Diskutiert wurden vor allem neue Aufgaben und Tätigkeitsbereiche von Aufsichtsbehörden im Rahmen der der neuen EU-Digitalrechtsakte sowie spezifische Fragestellungen im Datenschutzrecht. Am 10. Dezember 2025 erfolgte ein Besuch der DSB in Bratislava, in dessen Rahmen Fragestellungen bei der Verfahrensführung besprochen und Fallbeispiele aus der Entscheidungspraxis der slowakischen Aufsichtsbehörde und der DSB erörtert wurden.

Einen wichtigen Baustein im Bereich der bilateralen Kooperationen der DSB nimmt das jährliche Treffen mit den **mitteleuropäischen Datenschutz-Aufsichtsbehörden** von **Tschechien, Ungarn, Slowenien und der Slowakei** ein, das von der DSB erstmalig im Jahr 2024 initiiert und in Wien abgehalten wurde.[61] Aufgrund des großen Erfolges dieses Formats wurde ein regelmäßiger Austausch in diesem Format vereinbart. Das Treffen im Jahr 2025 wurde vom 15. bis 17. September 2025 von der ungarischen Aufsichtsbehörde unter Leitung von **Dr. Attila Péterfalvi** in Budapest veranstaltet und um die Teilnahme der **kroatischen Aufsichtsbehörde** erweitert. Die teilnehmenden Aufsichtsbehörden präsentierten die aktuellen Entwicklungen und Herausforderungen in ihren Mitgliedstaaten im Bereich Datenschutz und Informationsfreiheit. Für das Jahr 2026 wurde vereinbart, das Treffen in Slowenien abzuhalten.

Der **Bayerische Landesbeauftragte für den Datenschutz**, **Prof. Dr. Thomas Petri**, veranstaltet regelmäßig jährliche Treffen mit unterschiedlichen Aufsichtsbehörden. Die DSB folgte am 26. September 2025 einer Einladung zu einem informellen Treffen nach München, an dem auch die Aufsichtsbehörden von Tschechien und Malta teilnahmen.Am 25. November 2025 empfing die DSB in ihren Räumlichkeiten eine **Delegation aus Serbien** bestehend aus Mitgliedern der serbischen Aufsichtsbehörde für Datenschutz und Informationsfreiheit, des serbischen Innenministeriums sowie Vertreter:innen der OSZE-Mission in Serbien. Der Besuch der serbischen Delegation erfolgte im Rahmen des OSZE-geförderten Projekts “Consolidating the democratization process in the security sector in Serbia”[62]. Thematisch wurde ein weiter Bogen über die unterschiedlichen Tätigkeitsbereiche der DSB gespannt, wobei besonderes Augenmerk auf die datenschutzrechtliche Aufsicht über Strafverfolgungsbehörden gelegt wurde.

Schlussendlich empfing die DSB vom 17. bis 18. Dezember 2025 eine Delegation der **slowenischen Aufsichtsbehörde** unter Führung ihrer Leiterin und Vizevorsitzenden des EDSA **Dr.in Jelena Virant Burnik**. Im Rahmen dieses Treffens wurden Arbeitsgruppen aus den Bereichen Datenschutz, Informationsfreiheit und KI gebildet, um themenbezogene Fragestellungen effizient behandeln zu können.

Der bilaterale Austausch hat sich auch im Jahr 2025 für die DSB als ein wesentliches Instrument erwiesen, um für aktuelle und künftige Herausforderungen gewappnet zu sein, eigene Erfahrungen weiterzugeben bzw. neue Denkanstöße zu erhalten und ein wachsendes Netzwerk an Partnerbehörden aufzubauen. Aus diesen Gründen wird die DSB ihre bilateralen Kooperationen auch im Jahr 2026 weiterverfolgen und vertiefen.

---

61 Eine Zusammenfassung dieses Treffens ist Kapitel 7.1. des Jahresberichts 2025 zu entnehmen, siehe https://dsb.gv.at/sites/site0344/media/downloads/datenschutzbericht_2024.pdf.

62 Siehe https://serbia.osce.org/mission-to-serbia/580225.

8. Künstliche Intelligenz

8.1 KI-Verordnung - wesentliche Inhalte und Berührungspunkte zum Datenschutz

Mit der **Verordnung (EU) 2024/1689** vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (**KI-VO bzw. AI-Act**) hat die Europäische Union als weltweit erste politische und wirtschaftliche Akteurin einen **umfassenden, verbindlichen Rechtsrahmen für den Einsatz von künstlicher Intelligenz** geschaffen. Ziel der Verordnung ist es, Innovationen zu fördern, zugleich aber Grundrechte der betroffenen Personen zu schützen. Die KI-VO wurde am 12. Juli 2024 im Amtsblatt der Europäischen Union kundgemacht und trat am 20. Tag nach der Veröffentlichung in Kraft. Sie gilt grundsätzlich ab dem 2. August 2026, wobei die Regelungen zu verbotenen KI-Praktiken bereits seit 2. Februar 2025 gelten.

Der Kern der KI-VO besteht aus einem risikobasierten Ansatz, der KI-Systeme nach ihrem potenziellen Risiko einstuft:

- **Verbotene KI-Praktiken**: umfasst sind insbesondere Anwendungen, die Grundrechte erheblich beeinträchtigen (z. B. manipulative KI, Social Scoring, bestimmte Formen biometrischer Massenüberwachung).

- **Hochrisiko-KI-Systeme** unterliegen strengen Anforderungen. Dazu zählen v. a. KI-Anwendungen in den Bereichen Personalrekrutierung, Bildung, Gesundheitswesen, Strafverfolgung, Grenzkontrollen und Zugang zu öffentlichen Leistungen.

- **KI-Systeme mit begrenztem Risiko** unterliegen vor allem Transparenzverpflichtungen (v.a. die Kennzeichnung von KI-generierten Inhalten)

- **KI-Systeme mit minimalem Risiko** (z. B. einfache Assistenzsysteme) bleiben weitgehend unreguliert, die Compliance soll hier vor allem über gemeinsame Standards hergestellt werden

Für Hochrisiko-KI-Systeme schreibt die KI-VO umfassende Anforderungen an die Entwicklung, den Betrieb und die Nutzung vor. Dazu zählen insbesondere ein systematisches Risikomanagement, Vorgaben zur Qualität und zur Governance der verwendeten Daten, eine ausreichende technische Dokumentation sowie die Sicherstellung menschlicher Aufsicht. Ziel ist es, die Nachvollziehbarkeit, Sicherheit und Grundrechtskonformität dieser Systeme dauerhaft zu gewährleisten und mögliche Risiken für betroffene Person von Anfang an zu minimieren. In diesem Zusammenhang wird aktuell auf europäischer Ebene an Standards gearbeitet, mit welchen die Konformität nachgewiesen werden kann.

Überprüft wird die Einhaltung der KI-VO im Wesentlichen von **Marktüberwachungsbehörden**, welche von den Mitgliedsstaaten zu benennen sind.

Obwohl die KI-VO ihrem Wesen nach dem Bereich „Produktsicherheit“ zuzuordnen ist, steht sie in engem Zusammenhang mit der DSGVO und ergänzt diese punktuell, ohne sie zu ersetzen (**Art. 2**

Abs. 7 KI-VO). Beide Regelwerke sind **parallel anzuwenden**, wenn KI-Systeme personenbezogene Daten verarbeiten, etwa beim Training, beim Testen in sogenannten **„KI-Reallaboren" („Sandboxes")** oder im operativen Einsatz. Während die DSGVO die Rechtmäßigkeit der Datenverarbeitung sowie die individuellen Rechte betroffener Personen sicherstellt, setzt die KI-VO zusätzliche Anforderungen, v.a. im Hinblick auf die Datenqualität und den Schutz vor Diskriminierung. Enge Berührungspunkte bestehen insbesondere beim Umgang mit biometrischen Daten sowie bei der Gewährleistung der Nachvollziehbarkeit und Überprüfbarkeit KI-gestützter Entscheidungen.

8.2 Rolle der DSB nach der KI-VO - Art. 74 Abs. 8 und Art. 77 KI-VO

Datenschutz-Aufsichtsbehörden wie die DSB haben im Rahmen der KI-VO **mehrere Rollen**, teils **zwingend, teils fakultativ**, inne. Die DSB wurde einerseits als eine für den Schutz der Grundrechte zuständige Behörde benannt (Art. 77 KI-VO). Dies ändert das Mandat und den Aufgabenbereich der DSB nicht, welcher sich weiterhin aus der DSGVO ergibt, ermöglicht aber etwa zusätzliche Ermittlungsbefugnisse im Zusammenhang mit KI-Systemen. Diesbezüglich ist an mehreren Stellen in der KI-VO eine Zusammenarbeit zwischen den Datenschutz-Aufsichtsbehörden und den Marktüberwachungsbehörden vorgesehen.

Die DSB kann jedoch auch selbst als Marktüberwachungsbehörde benannt werden. Im Fall von **Art 74 Abs 8** KI-VOist eine Zuständigkeit der Datenschutz-Aufsichtsbehörden (oder einer Stelle, die über das gleiche Maß an völliger Unabhängigkeit verfügt) als Marktaufsichtsbehörden nach der KI-VO bereits im Text selbst zwingend vorgesehen. In diesem Zusammenhang hat die DSB auch selbst als notifizierte Stelle im Umfang von **Art. 43 Abs. 1 UAbs. 2KI-VO** zu agieren. Die DSB würde in diesem Bereich selbst Konformitätsbewertungen von KI-Systemen durchführen. Ebenfalls sind mehrfach Meldepflichten an die Datenschutz-Aufsichtsbehörden vorgesehen (vgl **Art. 5 Abs 4, Art. 26 Abs 10, Art. 57 Abs 10**).

8.3 Umsetzung KI-VO in Österreich

Die Zuständigkeit für die Umsetzung der KI-VO in Österreich liegt beim Bundeskanzleramt. Ein Entwurf eines Durchführungsgesetztes, in dem auch die Marktüberwachungsbehörden mit ihren jeweiligen Zuständigkeitsbereichen konkret benannt werden, steht zum Zeitpunkt des Redaktionsschlusses noch aus. Die DSB steht diesbezüglich in regelmäßigem Austausch, sowohl mit dem Bundeskanzleramt und dem Bundesministerium für Justiz, als auch mit anderen potentiellen Marktüberwachungsbehörden. Aktuell nimmt die DSB in mehreren **Untergruppen des KI-Gremiums/AI Boards (Art. 65 KI-VO)** teil. Dazu zählen die Gruppen zu **Prohibitions, High-risk, Law Enforcement, Transparency** sowie **Market surveillance authorities (ADCO)**.

9. Transparenz und Targeting in der politischen Werbung

9.1 Umsetzung in Österreich - Pol-W-G

Die **VO (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung** (Targeting-VO)[63] gilt (vollumfänglich) seit dem 10. Oktober 2025. Die Verordnung legt harmonisierte Vorschriften für ein hohes Maß an Transparenz in Bezug auf politische Werbung und damit verbundene Dienstleistungen fest.

Zum Berichtszeitpunkt liegt ein Vorschlag für ein **Bundesgesetz über die Transparenz und das Targeting politischer Werbung zur Durchführung der Taargeting-VO und damit verbunden eine Novelle des KommAustria-Gesetzes sowie des Mediengesetzes (Pol-W-G)**,[64] vor.

Als zuständige Behörde gemäß **Art. 22 Abs. 3 und Abs. 4 sowie Art. 21 Abs. 4 Targeting-VO** wird die **Kommunikationsbehörde Austria** (KommAustria) vorgesehen. Die KommAustria ist darüber hinaus für die Verfolgung der in § 6 des Bundesgesetzes genannten Verwaltungsübertretungen zuständig.

Da auch die DSB teilweise für die Targeting-VO zuständig ist (hierzu sogleich), sieht das Bundesgesetz eine **Behördenkooperation** sowie einen regelmäßigen Erfahrungs- und Meinungsaustausch zwischen KommAustria und DSB vor. Für die Erfüllung der neuen Aufgaben der DSB werden unter § 7 des Bundesgesetzes Sonderbestimmungen zu Verfahren der DSB normiert.

9.2 Rolle der DSB

In **Art. 22 Abs. 1 Targeting-VO** ist eine **unmittelbare Zuständigkeit der DSB** als Aufsichtsbehörde für die Überwachung und Durchsetzung von Art. 18 und Art. 19 der Targeting-VO vorgesehen.

Konkret sehen diese Bestimmungen spezielle Pflichten für das **Targeting und die Anzeigenschaltung im Zusammenhang mit politischer Werbung** im Internet vor. Hervorzuheben ist, dass derartige Anzeigeschaltungen (und die damit verbundene Verarbeitung personenbezogener Daten) 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).

Für die Überwachung und Durchsetzung dieser Bestimmungen gelten die **Untersuchungs- und Abhilfebefugnisse der DSB gemäß Art. 58 DSGVO sinngemäß (Art. 22 Abs. 1 Targeting-VO)**.

63 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202400900, abgerufen am 18.02.2026.

64 https://www.parlament.gv.at/gegenstand/XXVIII/ME/49?selectedStage=100, abgerufen am 18.02.2026.

Auf die Maßnahmen nach **Art. 18 und 19 der Targeting-VO** findet das Kapitel VII der DSGVO zur Zusammenarbeit und Kohärenz ebenfalls Anwendung.

Ausdrücklich normiert wird außerdem, 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**).

Die bereits bestehende Judikatur des EuGH zur Auslegung von Art. 83 DSGVO (insbesondere im Zusammenhang mit der unmittelbaren Strafbarkeit juristischer Personen)[65] kann somit auch auf die Sanktionsnormen der Targeting-VO übertragen werden.[66]

Damit wird das bestehende datenschutzrechtliche Sanktionsregime der DSB nach Art. 83 DSGVO auf den Bereich der politischen Werbung ausgeweitet und die Durchsetzung zentraler Transparenz- und Schutzvorgaben der Verordnung sichergestellt.

Diese Sanktionen müssen unter Berücksichtigung der Umstände im Einzelfall wirksam, verhältnismäßig und abschreckend sein. Zudem müssen auch die in Art. 83 Abs. 2 DSGVO genannten Kriterien berücksichtigt werden.

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

Der Unionsgesetzgeber weist im **Erwägungsgrund 94 der Targeting-VO** ausdrücklich darauf hin, dass die DSB als unabhängige Aufsichtsbehörde dabei unterstützt werden sollte, ihre Befugnisse nach der DSGVO in vollem Umfang nutzen zu können, um den Schutz der personenbezogenen Daten sicherzustellen. Dem Zeitraum vor bevorstehenden Wahlen wird in Bezug auf die politische Meinungsbildung der Bürger:innen und der Ausübung ihres Wahlrechts besondere Bedeutung beigemessen.

Verstöße im Zeitraum vor Wahlen sind demnach besonders heikel und haben schwerwiegende Auswirkungen auf die Rechte der Betroffenen. Abhilfemaßnahmen müssen noch vor dem Wahltermin getroffen werden, um wirksam zu sein. Die DSB soll daher in dieser kritischen Zeit vor der Stimmabgabe im Rahmen einer Wahl sicherstellen, dass sie auch in der Lage ist, unverzüglich zu handeln, um die Rechte der Betroffenen zu schützen.

Für diese zusätzliche Aufgaben wurden der DSB jedoch bis dato keine weiteren Ressourcen zur Verfügung gestellt.

---

65 Vgl. EuGH 05.12.2023, C-807/21; 05.12.2023, C-683/21; 13.02.2025, C-383/23.

66 Siehe auch Erläuterungen zu 49/ME XXVIII. GP, S. 10f zu § 7.

10. Informationsfreiheit

10.1 Rolle der DSB - § 15 IFG

Mit 1. September 2025 sind **Art. 22a idF BGBl. I Nr. 5/2024** sowie das **Informationsfreiheitsgesetz (IFG), BGBl. I Nr. 5/2024**, in Kraft getreten.

Die Verpflichtungen nach dem IFG treffen die Datenschutzbehörde in mehrfacher Hinsicht: Einerseits ist sie selbst informationspflichtiges Organ, andererseits wurden ihr in **§ 15 IFG** zusätzliche, spezifische Aufgaben übertragen. Eine dieser Aufgaben ist die Beratung und Unterstützung der informationspflichtigen Stellen in datenschutzrechtlichen Belangen der Vollziehung der Informationsfreiheit durch die **Bereitstellung von Leitfäden und Angeboten zur Fortbildung** (siehe hierzu Punkt 10.2). Eine weitere Aufgabe der DSB ist die gemäß **§ 15 Abs. 2 IFG** vorgesehene **Evaluierungspflicht** (siehe dazu die Ausführungen unter Punkt 10.3).

Als informationspflichtiges Organ hat sich die DSB in den vergangenen Monaten mit den Verpflichtungen nach dem IFG auseinandergesetzt. Darüber hinaus sind bei der DSB seit 1. September 2025 insgesamt **25 Anträge auf Zugang zu Informationen** eingegangen. In drei Fällen wurde jeweils ein (bereits rechtskräftiger) Bescheid erlassen.

Darüber hinaus hat die DSB die nunmehr bestehende **proaktive Informationspflicht** zum Anlass genommen, ihre bereits auf Grundlage von **§ 23 Abs. 2 DSG** bestehende Pflicht zur Veröffentlichung von Entscheidungen grundsätzlicher Bedeutung auszuweiten und Entscheidungen, an denen ein Interesse für die Allgemeinheit besteht, im **RIS**[67] zu veröffentlichen. Auch wurden beispielsweise erstmalig die Fragenkataloge der in den vergangenen Jahren von der DSB durchgeführten Schwerpunktprüfungen auf **data.gv.at**[68] veröffentlicht.

10.2 Bereitstellung von Leitfäden und Angebote zur Fortbildung in datenschutzrechtlichen Belangen - § 15 Abs. 1 IFG

Vor allem in der ersten Jahreshälfte 2025 hat sich die DSB dieser Aufgabe intensiv gewidmet und einen umfangreichen und bereits vielfach zitierten Leitfaden[69] erarbeitet, der auf der Webseite der DSB abrufbar ist. Dieser soll als **„lebendes Dokument"** laufend ergänzt und um die sich künftig entwickelnde Rechtsprechung erweitert werden. Begleitend dazu wurden in den Monaten vor Inkrafttreten des IFG insbesondere **in allen neun Bundesländern sowie an drei Terminen an der Verwaltungsakademie des Bundes Schulungen für Bundes-, Landes- und Gemeindebedienstete** abgehalten, um Bedienstete der öffentlichen Verwaltung auf die datenschutzrechtlichen Aspekte im Zusammenhang mit der Informationsfreiheit vorzubereiten.

67 https://www.ris.bka.gv.at/, abgerufen am 17.02.2026.
68 https://www.data.gv.at/home?locale=de, abgerufen am 17.02.2026.
69 https://dsb.gv.at/sites/site0344/media/downloads/leitfaden_ifg_-_stand_30.6.2025.pdf

Im Jahr 2026 werden zwei Schulungen an der Verwaltungsakademie des Bundes stattfinden. Darüber hinaus hat die DSB auch wesentliche „Fragen & Antworten“ zum Thema „Datenschutz & Informationsfreiheit“ ausgearbeitet und auf ihrer Webseite eröffentlicht.

10.3 Evaluierung des IFG - § 15 Abs. 2 IFG

Im Hinblick auf ihre Evaluierungsaufgabe, hat sich die DSB in der ersten Jahreshälfte 2025 mit europäischen Informationsfreiheitsbehörden, die ebenfalls einen entsprechenden Auftrag zur Evaluierung der dortigen Informationsfreiheitsgesetze haben, ausgetauscht. Darauf basierend wurden **internationalen Evaluierungsstandards entsprechende Kriterien** erarbeitet, anhand derer die DSB erstmals im Jahr 2026 eine Evaluierung für den **Berichtszeitraum 1. September bis 31. Dezember 2025** durchgeführt hat. Dabei ist das Ziel, auch zukünftig möglichst aussagekräftiges Datenmaterial zu erhalten, auf dessen Basis allfällige weitere Entscheidungen getroffen werden können.

Im Laufe des Jahres 2026 ist geplant, auf Grundlage der ersten praktischen Erfahrung mit der Evaluierung auch den Evaluierungsprozess einer umfassenden Bewertung zu unterziehen.

10.3.1 Evaluierung im Berichtszeitraum 1. September bis 31. Dezember 2025

Eingangs ist darauf hinzuweisen, dass die DSB Schätzungen zufolge davon ausgeht, dass rund 10.000 Stellen dem IFG unterliegen.[70] Davon haben jedoch nur **615 informationspflichtige Stellen** über das auf JustizOnline bereitgestellte Einmeldeformular eine **Meldung an die DSB**[71] erstattet. Generalisierende Aussagen oder die Ableitung belastbarer Trends sind daher derzeit nur eingeschränkt möglich. Der vorliegende Bericht kann jedoch erste Einblicke in die bisherige Anwendung des IFG geben und soll zur Information der Öffentlichkeit beitragen.

Von diesen 615 Stellen wurden insgesamt **8.236 eingegangene Anträge**[72] nach dem IFG gemeldet. Dabei handelt es sich um die Gesamtanzahl aller gemeldeter Anfragen und zwar unabhängig davon, ob diese **mündlich oder schriftlich** gestellt wurden.

10.3.1.1 Auswertung nach Organisationsbereichen

Die Auswertung nach Organisationsbereichen zeigt folgende Verteilung:

Im Bereich der **Bundesverwaltung** (einschließlich monokratischer Justizverwaltung) wurde von 45 Stellen eine Gesamtanzahl von **2.364 Anträgen** gemeldet. Spitzenreiter war das Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz mit 581 Anträgen, gefolgt vom Bundesministerium für Finanzen mit 203 Anträgen und dem Bundesministerium für Inneres mit 188 Anträgen.

Im Bereich der **Gemeinden** wurde von 288 Gemeinden eine Meldung abgegeben, insgesamt wurden **1.914 Anträge** gemeldet. Mit 943 Anträgen wurden die meisten Anträge von der Gemeinde

70 Die informationspflichtigen Stellen ergeben sich aus Art. 22a Abs. 1 bis 3 B-VG iVm. § 1 IFG.

71 Berücksichtigt werden konnten ausschließlich jene Meldungen, die über das auf JustizOnline bereitgestellte Einmeldeformular gemeldet wurden.

72 Eine entsprechende Differenzierung wurde den einmeldenen Stellen im Einmeldeformular auf JustizOnline optional freigestellt, lediglich bei der Angabe der Gesamtzahl handelte es sich um ein Pflichtfeld. Im Rahmen der Auswertung konnte festgestellt werden, dass die Zahl der gemeldeten, mündlichen Anfragen vernachlässigbar ist und wohl davon auszugehen ist, dass die einmeldenen Stellen mehrheitlich ausschließlich schriftliche Anfragen an die DSB gemeldet haben.

Wien (zusammengefasst Gemeinde und Landesverwaltung) gemeldet, gefolgt von der Landeshauptstadt Klagenfurt am Wörthersee mit 91 Anträgen und der Marktgemeinde Gröbming mit 84 Anträgen.

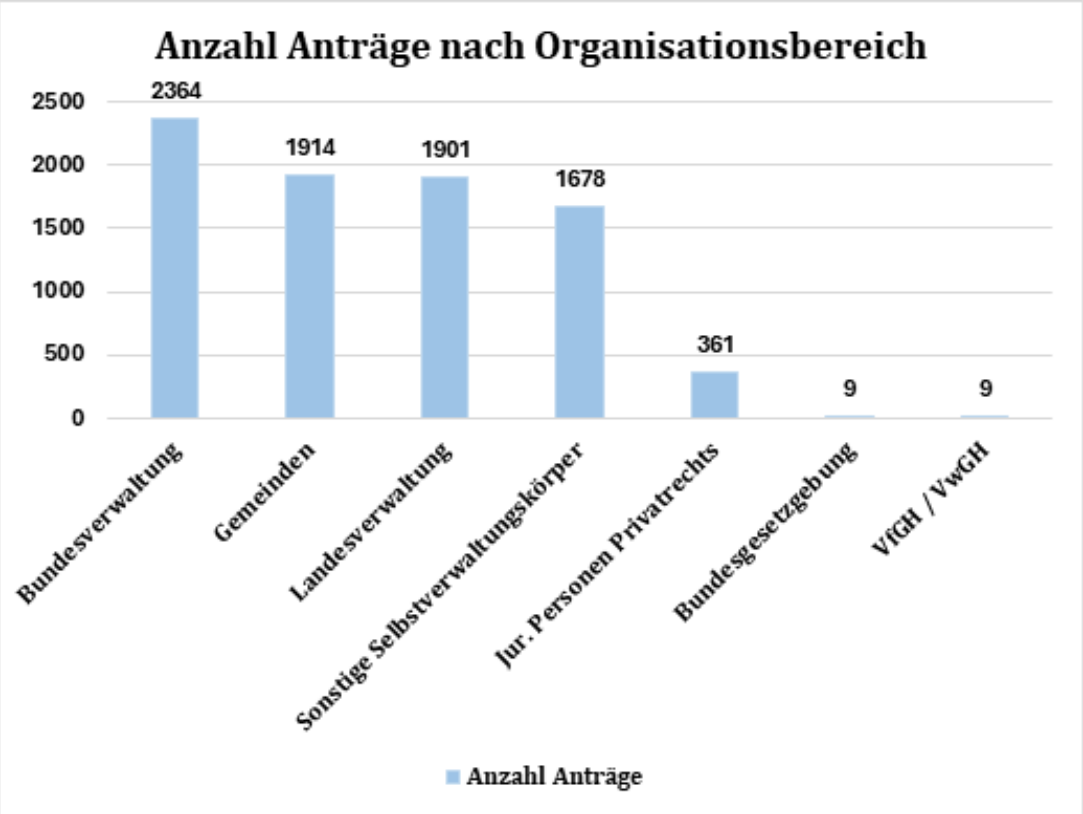
In der Kategorie informationspflichtige „**juristische Personen des Privatrechts**“ haben 186 Stellen eine Meldung abgegeben, insgesamt wurden von diesen **361 Anträge** gemeldet.

In Bereich der **Landesverwaltung** (einschließlich monokratischer Justizverwaltung) wurde von 28 Stellen eine Gesamtanzahl von **1.901 Anträgen** gemeldet. Davon wurden mit 465 Anträgen die meisten Anträge vom Land Niederösterreich gemeldet, gefolgt vom Land Steiermark mit 322 Anträgen, dem Land Vorarlberg mit 202 Anträgen und dem Land Tirol mit 201 Anträgen.

Im Bereich der **sonstigen Selbstverwaltungskörpern** haben 63 Stellen eine Meldung abgegeben, insgesamt wurden **1.678 Anträge** gemeldet.

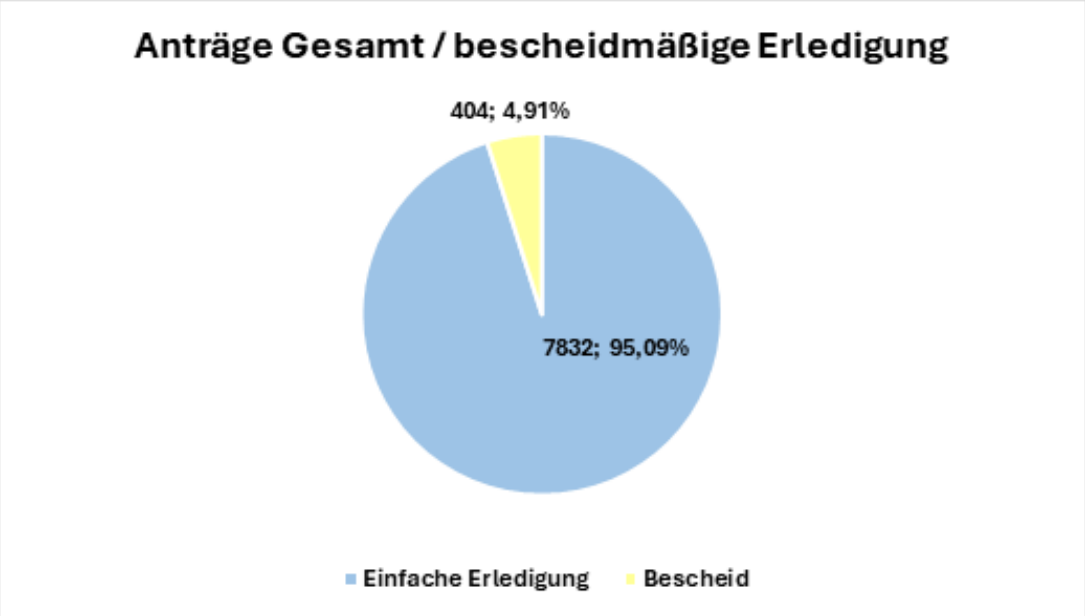
In der Kategorie **Organe der Bundesgesetzgebung** wurde von 3 Stellen eine Gesamtanzahl von **9 Anträgen** gemeldet

Auch der **Verfassungs- und Verwaltungsgerichtshof** haben jeweils eine Meldung abgegeben und insgesamt **9 Anträge** gemeldet.



10.3.1.2 Bescheide gemäß §11 Abs. 1 IFG

Von den 8.236 gemeldeten Anträgen wurden lediglich **404 Anträge (4,9 %) mit Bescheid erledigt.** Eine Erledigung mit Bescheid ist gemäß § 11 Abs. 1 IFG in jenem Fall vorgesehen, in welchem der **Zugang zur Information nicht gewährt wird und ein schriftlicher Antrag** der informationswerbenden Person an das informationspflichtige Organ gestellt wird.



Die meisten bescheidmäßigen Erledigungen wurden aus dem Bereich der **Gemeinden** gemeldet, und zwar **185 Bescheide** bei 1.914 gemeldeten Anträgen.

Im Bereich der **Bundesverwaltung** wurden von 2.364 gemeldeten Anträgen **102 Anträge bescheidmäßig erledigt.**

Im Bereich der **Landesverwaltung** wurden von den 1.901 Anträgen 8**5 bescheidmäße Erledigungen** gemeldet.

Von den informationspflichtigen sonstigen Selbstverwaltungskörpern wurden von 1.678 Anträgen 32 bescheidmäßige Erledigungen gemeldet.

In der Kategorie **Organe der Bundesgesetzgebung** sowie von Verfassungs- und Verwaltungsgerichtshof wurde **keine Bescheiderlassung gemeldet.**

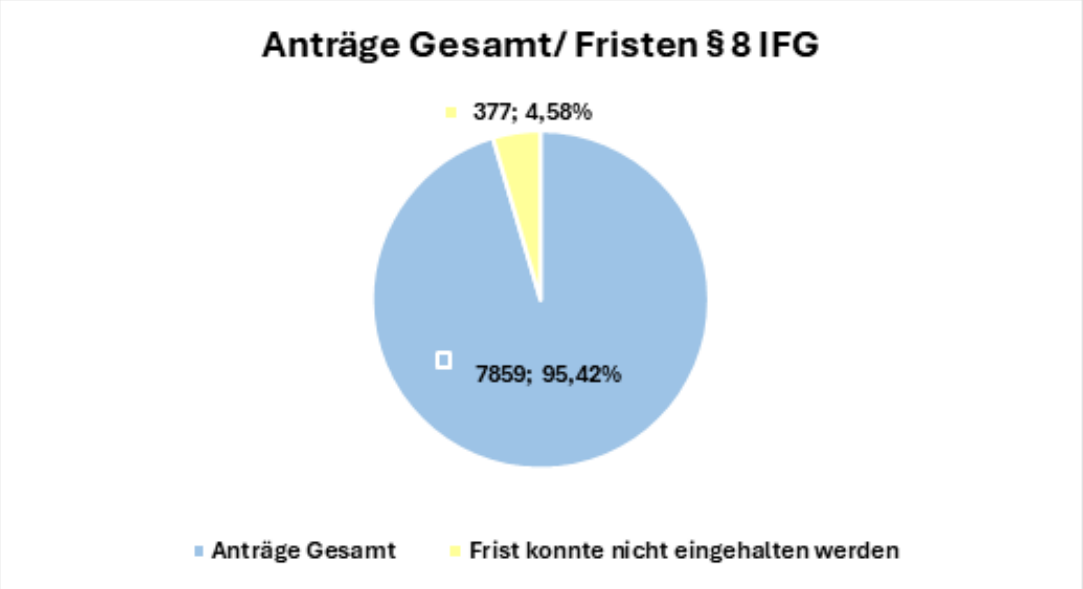
Insgesamt zeigt sich daher, dass Anträge auf Zugang zu Informationen **überwiegend ohne formale Bescheiderlassung erledigt** werden.

10.3.1.3. Einhaltung der Fristen

Es ist zunächst darauf hinzuweisen, dass es sich bei der im Rahmen von JustizOnline vorgesehenen Angabe zur Einhaltung der Fristen um kein verpflichtendes Eingabefeld gehandelt hat. Dementsprechend wurde nicht von allen Stellen, die eine Meldung an die DSB erstattet haben, eine Angabe zur Einhaltung der Fristen gemacht.

Von den 8.236 gemeldeten Anträgen wurde zu **377 Fällen** angegeben, dass die gemäß § 8 IFG vorgesehenen Fristen nicht eingehalten werden konnten.

Als Gründe wurden sowohl die **Anzahl der Anfragen, mangelnde Ressourcen sowie Umfang und Komplexität der Anfrage** genannt.



Die Auswertung nach Organisationsbereichen zum Thema Fristen zeigt folgende Verteilung:

Organisationsbereich	Gemeldete Anträge gesamt	Frist nicht eingehalten
Bundesverwaltung[73]	2.364	147
Gemeinden	1.914	181
Landesverwaltung[74]	1.901	0
Organe der Bundesgesetzgebung	9	0
Verfassungsgerichtshof und Verwaltungsgerichtshof	9	0
Sonstige Selbstverwaltungskörper	1.678	11
Juristische Personen des Privatrechts	361	38
GESAMT	**8.236**	**377**

73 Einschließlich monokratischer Justizverwaltung.
74 Einschließlich monokratischer Justizverwaltung.

10.3.1.4 Schlussbemerkungen

Insgesamt lässt sich für den Berichtszeitraum vom 1. September 2025 bis 31. Dezember 2025 beobachten, dass sich das **Informationsinteresse auf den Bereich der Bundes- und Landesverwaltung konzentriert**, was sich in höheren Fallzahlen pro Stelle widerspiegelt. Die Auswertung zeigt ebenfalls, dass sich im Bereich der Gemeinden der Großteil der Anfragen auf eine verhältnismäßig geringe Anzahl von Gemeinden fokussiert, weshalb die durchschnittliche Fallzahl ebenfalls gering ausfällt.

Im Folgenden ein Gesamtüberblick:[75]

Organisationsbereich	Anzahl Stellen	Anzahl Anträge	Anzahl Bescheide	Anträge pro Stelle	Bescheid-Quote
Bundesverwaltung[76]	45	2.364	102	52,5	4,31%
Gemeinden	288	1.914	185	6,6	9,67%
Landesverwaltung[77]	28	1.901	85	67,9	4,47%
Organe der Bundesgesetzgebung	3	9	0	3	0,00%
Verfassungs- und Verwaltungsgerichtshof	2	9	0	4,5	0,00%
Sonstige Selbstverwaltungskörper	63	1.678	32	26,6	1,91%
Juristische Personen des Privatrechts	186	361	--	1,9	0,00%
GESAMT	**615**	**8.236**	**404**	**13,4**	**4,91%**

75 Einschließlich monokratischer Justizverwaltung.
76 Einschließlich monokratischer Justizverwaltung.
77 Einschließlich monokratischer Justizverwaltung.

11. Plattformarbeit

Der Begriff Plattformarbeit bezeichnet Arbeitsformen, bei denen **digitale Plattformen als Vermittler zwischen Auftraggeber:innen und Arbeitskräften** auftreten. Die Organisation, Zuteilung und Bewertung der Arbeit erfolgen dabei meist algorithmisch, etwa über Apps oder Online-Portale. Typische Merkmale sind flexible Arbeitszeiten, eine starke Individualisierung der Aufträge und häufig unsichere Beschäftigungsbedingungen, da viele Plattformbeschäftigte formal als Selbstständige gelten bzw. wie solche behandelt werden. Heute hat Plattformarbeit vor allem in Bereichen wie Personenbeförderung, Essenszustellung, Haushaltsdienstleistungen oder digitaler Wissensarbeit stark an Bedeutung gewonnen und prägt zunehmend den Arbeitsalltag vieler Menschen.

Laut einer Analyse der Arbeiterkammer arbeiteten im Jahre 2024 360.000 Personen in Österreich über Plattformen, EU-weit waren es ca. 43 Millionen Personen[78].

In Zukunft ist davon auszugehen, dass Plattformarbeit weiter zunimmt und sich auf weitere Branchen ausdehnt, etwa Pflege, Handwerk oder kreative Tätigkeiten. Damit steigt auch ihre gesellschaftliche und arbeitsmarktpolitische Relevanz, insbesondere im Hinblick auf soziale Absicherung, Mitbestimmung und faire Entlohnung. Eine zentrale Herausforderung liegt darin, vor dem Hintergrund von hochentwickelten Algorithmen zur Steuerung und Kontrolle den Schutz der personenbezogenen Daten der Plattformarbeitenden sicherzustellen.

11.1 Richtlinie Plattformarbeit - PlArbRL

Mit der **Richtline (EU) 2024/2831** vom 23. Oktober 2024 unternimmt der europäische Gesetzgeber erstmals Schritte, um den stark wachsenden Bereich der Plattformarbeit einer einheitlichen rechtlichen Regelung zu unterziehen. Die Ziele der RL bestehen dabei ausdrücklich darin, die Arbeitsbedingungen in der Plattformarbeit zu verbessern sowie den Schutz der personenbezogenen Daten der Plattformarbeit leistenden Personen zu gewährleisten. Die Mittel zur Erreichung der genannten Ziele bestehen einerseits in Maßnahmen zur Erleichterung der Bestimmung des korrekten Beschäftigungsstatus (Stichwort: Scheinselbständigkeit), andererseits aber auch in der Schaffung von Transparenz, Fairness, Aufsicht und Sicherheit beim algorithmischen Management der Plattformarbeit. Laut **Erwägungsgrund 38 der Richtlinie** soll diese hierbei im Vergleich zur DSGVO **spezifischere Vorschriften für den Einsatz und die Transparenz von automatisierten Entscheidungssystemen** festlegen. Zu diesem Zwecke werden in **Art. 7 der Richtlinie** konkrete Einschränkungen für die Verarbeitung von personenbezogenen Daten mittels automatisierter Beobachtungs- und Entscheidungssysteme normiert (zB das Verbot der Verarbeitung von Daten über den emotionalen Zustand einer Person, die Plattformarbeit leistet, oder von Daten über private Gespräche mit anderen Plattformarbeit leistenden Personen). Darüber hinaus unterliegen Betreiber von Plattformen im Sinne der RL **umfassenden Transparenzverpflichtungen** sowohl gegenüber Beschäftigten als auch gegenüber den zuständigen Behörden. Nicht unerwähnt bleiben soll an dieser Stelle auch die **Verpflichtung zur Erstellung einer Datenschutz-Folgenabschätzung** im Sinne des Art. 35 DSGVO.

78 https://ak-aktuell.at/themen/arbeit/plattformarbeit-ein-blick-ueber-den-tellerrand, abgerufen am 18.02.2026.

Eine weitere wichtige Komponente des Schutzes der Rechte und Freiheiten von Plattformarbeit leistenden Personen besteht in der **Verpflichtung zur menschlichen Aufsicht über automatisierte Bewertungs- und Entscheidungssysteme**. Derartigen Systemen unterworfene Beschäftigte sollen zudem das Recht haben, schriftliche oder mündliche Erklärungen über automatisierte Entscheidungen zu erhalten sowie die Überprüfung durch eine natürliche Person zu erwirken. Wie bei Art. 22 DSGVO besteht das Ziel dabei darin, dass Plattformarbeit leistende Person nicht zum Spielball intransparenter, vollautomatisierter Algorithmen werden sollen, deren Entscheidungen und Bewertungen nicht mehr nachvollzogen werden können.

Die Umsetzung der **RL 2024/2831** soll in Österreich im Wege eines **Bundesgesetzes über die Arbeit für digitale Arbeitsplattformen (Plattformarbeitsgesetz-PArbG)** erfolgen. Ein entsprechender Gesetzesentwurf befindet sich zum Zeitpunkt der Drucklegung dieses Berichts gerade unter Federführung des Bundesministeriums für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK) in Abstimmung zwischen den verschiedenen Stakeholdern.

11.2 Rolle der DSB

Sowohl die **RL 2024/2831** selbst, als auch das darauf aufbauende nationale Plattformarbeitsgesetz sehen eine **entscheidende Rolle für die DSB** beim Vollzug des Gesetzes und der darin bezweckten Sicherstellung des Schutzes der personenbezogenen Daten von Plattformarbeit leistenden Personen vor.

So normiert **Art. 24 Abs. 1 der Richtlinie** beispielweise die Zuständigkeit der Datenschutzbehörde für die **Überwachung der Einhaltung der Artikel 7 bis 11** unter Zugrundelegung der in den **Kapiteln VI, VII und VIII der DSGVO** vorgesehenen Bestimmungen. Die von der DSB zu beaufsichtigenden Bereiche bestehen v.a. in den Einschränkungen bei der Verarbeitung personenbezogener Daten mittels automatisierter Beobachtungs- und Entscheidungssysteme, in den Transparenzverpflichtungen der Plattformbetreiber sowie in der Sicherstellung der menschlichen Aufsicht bzw. der Möglichkeit des menschlichen Eingriffs in die genannten Systeme. Darüber hinaus wird die DSB auch für die **Sanktionierung von Verstößen** gegen die oben genannten Artikel zuständig sein. Der Strafrahmen soll sich dabei nach den Bestimmungen des **Art. 83 Abs. 5 DSGVO** richten. Abschließend ist jedoch festzuhalten, dass die Wirksamkeit der Richtlinie nicht nur klare und praxistaugliche (verfahrens)rechtliche Regelungen voraussetzt. Ebenso **entscheidend** ist eine **ausreichende personelle, organisatorische und finanzielle Ausstattung** der DSB, um die vorgesehenen Aufgaben tatsächlich erfüllen zu können.