**Deutscher Bundestag** **Drucksache 21/5950**

**21. Wahlperiode** 06.05.2026



# Unterrichtung

**durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit**

## 34. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit (Tätigkeitsbericht für das Jahr 2025)

*Zugeleitet mit Schreiben der Beauftragten für den Datenschutz und die Informationsfreiheit vom 6. Mai 2026 gemäß § 15 des Bundesdatenschutzgesetzes.*

# Inhaltsverzeichnis

# 1 Eingangsinterview mit Prof. Dr. Louisa Specht-Riemenschneider



*Quelle: Johanna Wittig*

**Louisa Specht-Riemenschneider, wie war 2025?**

2025 hatte datenschutzrechtlich viel zu bieten! Langweilig war uns nicht. Wir hatten einiges zu tun, etwa mit der Einführung der elektronischen Patientenakte (ePA) und mit einem großen Aufsichtsverfahren gegen einen Telekommunikationsdiensteanbieter. Am Ende stand ein insgesamt 45 Millionen Euro schweres Bußgeld. Die EUDI-Wallet treibt uns um, die Aufsichtsverlagerung im Sicherheitsbereich droht und ich könnte noch viele andere Dinge aufzählen wie den Digital-Omnibus. Besonders gefreut habe ich mich darüber, dass wir große Schritte in Richtung unserer Sandbox, dem ReguLab, gemacht haben, die wir Anfang 2026 gestartet haben. Wir haben unsere erste Veranstaltung zum Strategic Foresight im Gesundheitsbereich durchgeführt und entwickeln daraus jetzt Ideen zur Umsetzung der gewonnenen Erkenntnisse. Und wir haben begonnen, repräsentative Befragungen zu datenschutzrechtlich relevanten Themen durchzuführen. Auf Grundlage des Datenbarometers wollen wir die Politik noch besser beraten können. Ich glaube, dass wir als Aufsicht den Spagat zwischen gesetzlich möglicher Datennutzung und Innovationsförderung und dem hohen Schutz der Grundrechte der Bürgerinnen und Bürger schon ganz gut hinbekommen haben.

**Welche Fragen stellst Du Dir heute, die Du Dir zu Beginn Deiner Amtszeit als BfDI im Jahr 2024 noch nicht gestellt hast?**

Ich stelle mir nach einem Jahr in exekutiver Verantwortung stärker als zuvor die Frage nach der Effektivität des Rechts. So werden milliardenfach Daten rechtswidrig verarbeitet, zum Beispiel von Datenbrokern, die wir nicht zu fassen bekommen.

Wir brauchen eine Debatte darüber, wie wir das Datenschutzrecht effektiver gestalten können und dennoch Innovation, die dem Gemeinwohlinteresse dient, zulassen und fördern.

**Du hast 2025 angefangen, repräsentative Bevölkerungsumfragen durchführen zu lassen. Was ist da der Hintergedanke?**

Der Hintergedanke ist, dass wir als Regulierer vermeiden sollten, unseren Entscheidungen nur anekdotisches Wissen über die vermeintlichen Präferenzen der Menschen zum Thema Datenschutz zugrunde zu legen. Ich glaube, dass nicht nur wir, sondern auch der Gesetzgeber viel stärker mit Evidenz arbeiten sollte. Unsere Befragungen der Bevölkerung, aber auch unsere Gespräche mit NGOs, Behörden und Unternehmen zeigen immer wieder, dass die Menschen sich stärker für Datenschutz und datenschutzsensible Innovationen interessieren als oft behauptet wird – wenn sie angeboten werden.

**Kannst Du das an einem Beispiel festmachen?**

Wir wollten zum Beispiel wissen, was die Befragten mit Cookie-Manager-Diensten anfangen können. Für diese hatte die Politik große Pläne, aber die Einführung läuft schleppend. Ich kann mir vorstellen, dass das anders verlaufen wäre, wenn wir früher nachgefragt hätten,

ob Verbraucherinnen und Verbraucher darin einen Mehrwert sehen und sich überhaupt vorstellen können, solche Dienste damit zu beauftragen, ihre Datenschutz-Präferenzen gegenüber digitalen Diensten durchzusetzen. Die gute Nachricht ist, es gibt durchaus Interesse in der Bevölkerung: Zwei Drittel der Befragten können sich die Nutzung von Einwilligungsmanagern gut vorstellen. Das sollte ein Appell an die Politik sein, die Einführung solcher Dienste weiterhin ehrgeizig voranzutreiben und die rechtlichen Rahmenbedingungen hierfür zugunsten der Verbraucherinnen und Verbraucher zu schärfen. Wir stehen als Partner bereit dafür.

**Was gab es außer diesen Projekten Neues bei der BfDI?**

Wir befinden uns mitten in einem Change-Prozess. Ziel ist, das neue Leitbild des Hauses mit Leben zu füllen. Das heißt, dass wir mehr auf proaktive Beratung zu Datenschutzthemen setzen und uns für die aktuellen Herausforderungen effizient aufstellen, insbesondere durch ein Referat für Bürgerdialog und ein zentrales Beschwerdemanagement zur zügigen Bearbeitung von Eingaben, vor allem Beschwerden. Wir erhalten nämlich immer mehr Eingaben, darunter Beschwerden von Bürgerinnen und Bürgern. 2023 hatten wir rund 7 800 Eingaben, davon etwa 2 500 formelle Beschwerden. Im Jahr 2025 hatten wir fast 12 000 Eingaben, darunter gut 5 300 Beschwerden. Die Eingaben sind also um rund 54 Prozent gestiegen, die Beschwerden haben sich in zwei Jahren sogar mehr als verdoppelt. Unser Anspruch bleibt dabei, die Rechte der Bürgerinnen und Bürger auch in Zukunft weiter effektiv durchzusetzen. Das ist – wie gesagt – ein Prozess, und er wird noch eine Weile dauern. Ich bin überzeugt, dass unser Beratungsansatz richtig ist, um für mehr datenschutzkonforme Gesetze, Produkte und Dienstleistungen zu sorgen.

Positive Erfahrungen konnten wir zum Beispiel auch im Rahmen des von uns neu aufgesetzten Health Foresight machen: Wir haben verschiedene Akteure aus Wissenschaft, Politik, Wirtschaft und Verwaltung eingeladen, um über ausgewählte Zukunftsthemen der Medizin zu diskutieren. Als Aufsichtsbehörde konnten wir viel zu spannenden Themen wie Neurodaten, Gehirn-Computer-Schnittstellen, Schwarmlernen und Human Enhancement lernen. Wusstest Du zum Beispiel, dass die Medizin inzwischen in der Lage ist, querschnittsgelähmten Menschen über Neurodaten die Steuerung von Computern zu ermöglichen oder gar zu laufen? Diese Möglichkeit darf Datenschutz nicht abschneiden, und dennoch müssen wir den Gefahren begegnen, die mit einer möglichen unrechtmäßigen Verwendung dieser Daten einhergehen. Diese und weitere Erkenntnisse können wir nun an den Gesetzgeber weitergeben, wenn es perspektivisch an die konkrete Regulierung dieser Felder geht, und werden sie natürlich auch im Rahmen unserer Aufsichts- und Beratungstätigkeit anwenden.

**Was gibt es Neues beim Thema Künstliche Intelligenz aus Sicht des Datenschutzes?**

Natürlich stellen große Sprachmodelle für den Datenschutz eine große Herausforderung dar. Denn bewährte Prinzipien des vor fünfzig Jahren entwickelten Datenschutzrechts wie Transparenz, Zweckbindung und Rechenschaftspflicht sind von grundlegend anderen Datenverarbeitungen ausgegangen, als wir sie bei Künstlicher Intelligenz vorfinden. Es ist die große Frage unserer Zeit, wie wir den Trade-off zwischen Nutzung der Chancen von KI, die ein Stück weit nicht komplett nachvollziehbar ist, auf der einen Seite und der Wahrung datenschutzrechtlicher Grundfesten auf der anderen Seite ausverhandeln. Aber das sollte uns ein Ansporn sein, dafür Lösungen zu finden, statt eine in vielen Kontexten nützliche Technologie per se in die Schmuddelecke zu stellen. Ich begleite die Entwicklung und den Einsatz von KI gemeinsam mit meinem Haus deshalb aktiv. In einem Konsultationsverfahren haben wir gemeinsam mit Akteuren aus Wissenschaft, Wirtschaft, Verwaltung und Zivilgesellschaft datenschutzrechtliche Lösungen für die Entwicklung und den Einsatz von KI entwickelt, insbesondere was Rechtsgrundlagen und die Durchsetzung von Betroffenenrechten angeht. Basierend auf diesen Erkenntnissen konnten wir auch einen Leitfaden für die Nutzung von KI in Bundesbehörden herausgeben, der sehr positiv aufgenommen wurde.

**Es lief aber 2025 auch nicht alles glatt, oder?**

Zur Ehrlichkeit gehört dazu, dass beispielsweise ein Gerichtsverfahren zwischen meiner Behörde und dem Presse- und Informationsamt der Bundesregierung nicht zu meiner Zufriedenheit ausgegangen ist. Ich möchte hier sehr deutlich klarstellen, dass es meiner Behörde nicht darum geht, der Bundesregierung die Nutzung sozialer Medien zu verbieten. Ganz im Gegenteil sehe auch ich, dass soziale Medien relevant sind, um Menschen zu erreichen. Es geht vielmehr darum, dass Bürgerinnen und Bürger sich darauf verlassen können müssen, dass dann, wenn der Staat soziale Medien nutzt, kein Schindluder mit ihren Daten getrieben wird. Deshalb streiten wir dafür, dass die Plattformen, deren Angebot der Staat zur Wahrung der öffentlichen Informationspflicht nutzt, das geltende Recht achten.

**Wie würdest Du die Stimmung in der Datenschutz-Szene aktuell beschreiben?**

Ich nehme viele Bedenken und Sorgen wahr, etwa was das unregulierte Agieren von Datenbrokern angeht. Ebenso Sorgen mit Blick auf IT-Sicherheit und digitale Souveränität. Mitte 2025 wurde auch meine Handynummer zum Gegenstand von unerlaubtem Datenhandel, neben derjenigen von unserem Bundeskanzler, Kabinettsmitgliedern und führenden Militärs. Ich kann sagen: Das ist kein schönes Gefühl und bestärkt mich, in diesem Bereich weiter für eine strengere Regulierung und vor allem eine bessere Rechtsdurchsetzung einzustehen.

Ich nehme aber in vielen Teilen der Datenschutz-Community auch einen starken Wunsch nach Differenziertheit wahr. Die Erzählung von den ewig bremsenden Datenschützern ist falsch. Daher habe ich aktiv im Europäischen Datenschutzausschuss den sogenannten Helsinki-Prozess mit vorangetrieben. Dort haben wir europaweit vereinbart: Wir müssen es denen, die Datenschutz von Anfang an einhalten wollen, einfacher machen. Mir war es persönlich ein Anliegen, dass wir in ganz Europa gerade KMU mit Checklisten und ,,how to"-Papieren unter die Arme greifen. Das wird nicht reichen, aber es ist ein Anfang. Es geht darum, Innovation grundrechtskonform zu ermöglichen und dabei neben den Kurzfristvorteilen auch die Langfristrisiken zu sehen. Wie gehen wir mit der stetig wachsenden Macht von Algorithmen und Plattformen um? Was macht es mit uns als Gesellschaft, wenn wir nicht mehr selbst entscheiden, welche Inhalte wir wahrnehmen, oder wenn wir nicht mehr selbst erkennen, welche Inhalte echt und welche nur ein Fake sind? Es geht um den Schutz dieser Gesellschaft vor Manipulation und der Konzentration von Meinungsmacht. Es geht um nicht weniger als um die Gewährleistung von Sicherheit, Freiheit und Demokratie, zu der das Datenschutzrecht einen ganz großen Teil beitragen kann.

**Welche Gesetzgebungsverfahren siehst Du kritisch oder gespannt?**

Ganz oben auf der Liste stehen der Digital-Omnibus und der KI-Omnibus. Einige Ideen daraus unterstütze ich, andere nicht. Ich halte es etwa für richtig, Rechtsakte zu konsolidieren, sie besser auf einander abzustimmen. Ich kritisiere, dass viele sehr wichtige Dinge weder im Digital- noch im KI-Omnibus angegangen werden. Statt sich an Definitionen zu zerstreiten, sollte ein Fokus darauf gelegt werden, wie es tatsächlich gelingt, die Kontrolle über unsere Daten im Netz zurückzuerlangen. Und letztlich dürfen wir die Augen nicht verschließen vor Netzwerkeffekten, Machtasymmetrien, Informationsüberlastung und ihren Auswirkungen auf die Freiwilligkeit der Einwilligung. Zu all dem finde ich im Omnibus nichts.

Auf nationaler Ebene schaue ich mir ganz besonders gerne das Forschungsdatengesetz an. Als Wissenschaftlerin setze ich mich schon lange für eine datenschutzkonforme, sichere Datennutzbarkeit im Forschungs- und Wissenschaftsbereich ein. Das Forschungsdatengesetz bietet die Chance, endlich einen verbesserten Datenzugang für Forschende zu Zwecken des Allgemeinwohls zu gewähren, ohne dass das Datenschutzrecht geschwächt wird. In diesem Sinne blicke ich auch gespannt auf die Bestrebungen für ein Datengesetzbuch oder das Beschäftigtendatengesetz.

Sehr kritisch schaue ich natürlich auf die angedachten Reformen im Sicherheitsbereich. Die Reform des Bundespolizeigesetzes und des MAD-Gesetzes habe ich selbstverständlich konstruktiv-kritisch begleitet. Aber Sorgen bereiten mir die Pläne einer Verschiebung der Aufsicht über die Nachrichtendienste. Diese Reform wurde schon vor einigen Jahren politisch beschlossen, soll aber erst jetzt rechtlich umgesetzt werden. Das ist für den Grundrechtsschutz der Bürgerinnen und Bürger eine schlechte Nachricht, denn bislang habe ich mit meinem Haus einen Rundumblick über alle Datenverarbeitungen von Polizeien und Nachrichtendiensten des Bundes. Nur mein Haus weiß, welche Systeme auf Bundesebene insgesamt eingesetzt werden und kann der vom Bundesverfassungsgericht postulierten Kompensationsfunktion insgesamt gerecht werden.

Sollen Doppelkontrollen vermieden werden, wäre es viel einfacher und effektiver, die gesetzlichen Einschränkungen für inhaltlichen Austausch zwischen dem Unabhängigen Kontrollrat und meinem Haus abzubauen. Kontrollen des Bundesnachrichtendienstes könnten dann aufeinander abgestimmt werden.

Ich wehre mich mit Händen und Füßen gegen die Aufsichtsverschiebung. Aber mit Argumenten scheint man gegen einen einmal gefassten Beschluss – so absurd er auch sein mag – nicht mehr anzukommen. Es wäre die bislang größte Niederlage des Datenschutzrechts.

**Was wünschst Du Dir für 2026?**

Ich wünsche mir drei Dinge: Dass unsere Sandbox angenommen wird, dass Bürgerinnen und Bürger nicht eine Schwächung der Aufsicht über die Nachrichtendienste erleiden müssen und dass wir alle die Hoffnung nicht verlieren, dass Digitalisierung zum Wohle der Gesellschaft ausgestaltet werden kann.

Allen Leserinnen und Lesern wünsche ich nun viel Freude und Erkenntnisgewinn mit unserem Tätigkeitsbericht!

# 2 Schwerpunktprojekte



## 2.1 Technology Foresight und Strategic Foresight

**Ich habe den 2024 begonnenen Aufbau der Strategic Foresight fortgesetzt und im Berichtsjahr einen Schwerpunkt auf den Bereich Gesundheit gelegt. Zudem konnten in einem ersten Durchlauf von Technology Foresight sechs datenschutzrelevante Technologietrends identifiziert werden.**

### Technology Foresight

Der im März 2024 bei der BfDI etablierte „Technology Foresight" verfolgt das Ziel, die Datenschutzrelevanz neuer Technologietrends rechtzeitig zu identifizieren und diese anschließend nach den Datenschutzgrundsätzen gem. Art. 5 DSGVO in iterativen Phasen zu bewerten.[1] Im ersten Durchlauf des Technology Foresight hat die BfDI sechs datenschutzrelevante Technologietrends identifiziert:

1. Neurosymbolische Künstliche Intelligenz: ist eine Form der hybriden Künstlichen Intelligenz, die sowohl datengetriebenes als auch regelbasiertes Lernen kombiniert, wodurch sie potentiell die Transparenz der Ergebnisse im Vergleich zu reinem maschinellem Lernen erhöht. Gleichzeitig können mögliche Datenschutzrisiken durch eine potenzielle Re-Identifizierung trotz vorhergehender Anonymisierung personenbezogener Daten entstehen.
2. Topologisches Quantencomputing: Ein grundliegendes Problem in der Entwicklung leistungsfähiger Quantencomputer besteht darin, dass die verwendeten Qubits nicht stabil sind. Beim topologischen Quantencomputing werden Informationen in Qubits durch formgebende Eigenschaften geschützt. Das macht Qubits störunanfälliger, wodurch die Marktreife und damit die Datenschutzrelevanz zunehmend realistisch wird.
3. 6G-Mobilfunknetze: stellen die nächste, sechste Generation mobiler Funk-Kommunikation dar[2]. Angestrebt wird u. a. eine erweiterte Funktionalität durch die Kombination von Funk-Kommunikation und Funk-Sensorik in einer gemeinsamen Kommunikationsinfrastruktur (genannt JCAS – Joint Communication and Sensing), wodurch u. a. umfassende Umgebungsdaten inkl. personenbezogener Daten unbeteiligter Dritter erfasst werden können.
4. Extended Reality: bezieht sich auf ein breites Spektrum immersiver Technologien, die mithilfe von Hardware und Software interaktive Verbindungen zwischen den physischen und den virtuellen Welten herstellen. Die verwendeten Technologien sind i. d. R. tragbar und können in Kameras, Mikrofone und andere Sensoren verbaut sein, die umfassende Daten über die Nutzenden und die Umgebung sammeln, möglicherweise auch über unbeteiligte Dritte in der Umgebung.
5. Neurodaten: sind ein Sammelbegriff für Daten, die direkt aus der Gehirnaktivität gewonnen werden. Solche Daten bieten tiefe Einblicke in neuronale Prozesse und können charakteristische Muster bei neurologischen Erkrankungen wie Epilepsie aufzeigen und sind somit für die Diagnose neurologischer Erkrankungen gut geeignet.
6. Confidential Computing: bezeichnet den Einsatz vertrauenswürdiger Ausführungsumgebungen im Cloud-Kontext (Trusted Execution Environments), in denen Daten während der Verarbeitung (sog. Data-In-Use) vor unbefugtem Zugriff geschützt werden sollen.

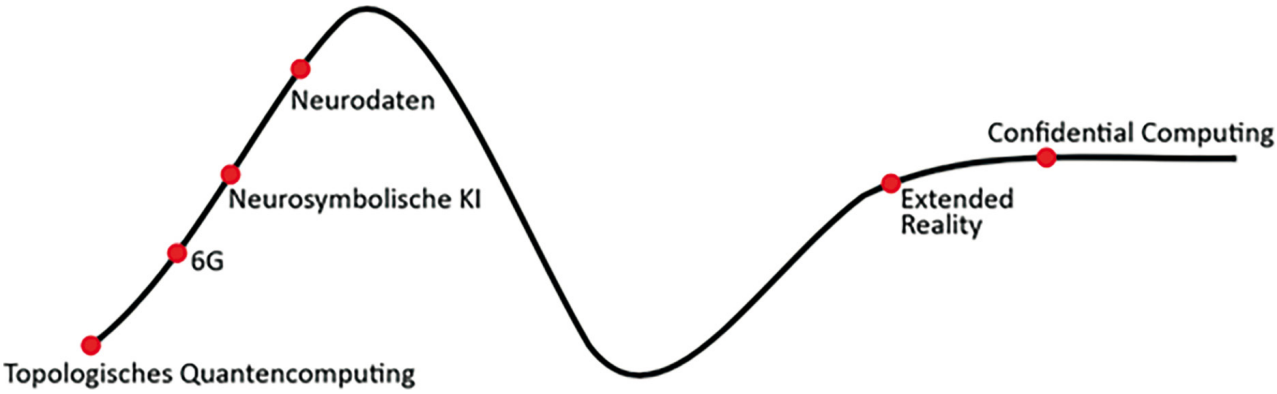
1 Vgl. 33. TB Nr. 9.5
2 Pressemitteilung der International Telecommunications Union (Dezember 2023), verfügbar unter: https://www.itu.int/en/mediacentre/Pages/PR-2023-12-01-IMT-2030-for-6G-mobile-technologies.aspx

Drei dieser identifizierten Technologietrends werden in Arbeitspapieren der Berlin Group thematisiert, nämlich Neurodaten, Extended Reality und Confidential Computing.

Ein weiterer Technologietrend mit maßgeblicher Datenschutzrelevanz ist der für 2030 angestrebte 6G-Mobilfunkstandard, welcher im Zusammenhang mit Technology Foresight in der 74. Sitzung der Berlin Group im November 2024 vorgestellt wurde[3]. Daraufhin hat die BfDI das Thema 6G für ein künftiges Arbeitspapier der Berlin Group aufgegriffen.

Erwähnenswert ist die Positionierung der zuvor genannten Technologietrends entlang eines „Hype-Zyklus“[4] aus Sicht des Datenschutzes. Während Topologisches Quantencomputing, 6G Mobilfunknetze und Neurosymbolische Künstliche Intelligenz am Anfang des Hype-Zyklus stehen, sind Extended Reality und Confidential Computing bereits marktreif. Diese Positionierung wird in der folgenden Abbildung aufgezeigt, angelehnt an den Gartner Hype Cycle™ für neue Technologien[5]:

**Technologietrends entlang eines Hype-Zyklus aus Sicht des Datenschutzes**




Diese Technologietrends, und insbesondere das Thema 6G, wurden im Rahmen eines Workshops mit Expertinnen und Experten im Berliner Verbindungsbüro der BfDI im November 2025 diskutiert. Ergebnis dieser Diskussionen waren neben wertvollen Inputs zu den o. g. Technologietrends auch die Identifizierung von zwei potenziellen Technologietrends für den zweiten Durchlauf des Technology Foresights, nämlich Agentische KI und Digitale Wallets. Solche Workshops mit der Betrachtung unterschiedlicher Perspektiven aus den Bereichen Politik, Verwaltung, Wissenschaft, Wirtschaft und Zivilgesellschaft auf dieselben Technologien sind ein zentraler Baustein des Technology-Foresight-Konzepts.

**Strategic Foresight**

Durch die Strategic Foresight in meinem Haus werden im Austausch mit Expertinnen und Experten und aufbauend auf den Ergebnissen des Technology Foresights fortlaufend in jährlichen Schwerpunktbereichen politisch-strategisch relevante Zukunftsthemen identifiziert und dazu datenschutzpolitische und rechtliche Positionen erarbeitet.[6] Durch datenschutzrechtliche Leitlinien und Handlungsempfehlungen sollen die Rechtssicherheit für Innovationen verbessert und datenschutzpolitische Optionen für die Rechtssetzung aufgezeigt werden.

Im Jahr 2025 habe ich einen Fokus auf den Bereich Gesundheit gelegt. Auf Grundlage der identifizierten Technologietrends habe ich mit meinem Haus herausgearbeitet, welche neuen Technologien und Innovationen im Bereich Gesundheit in der Zukunft besonders relevant werden könnten und welche datenschutzrelevanten Herausforderungen und Lösungsansätze bestehen oder zu erarbeiten sind. Bei einer Veranstaltung im Oktober 2025 diskutierten ca. 50 Teilnehmerinnen und Teilnehmer anhand von Expertenvorträgen über folgende Innovationsansätze: neue Formen maschi-

3 Vgl. 33. TB Nr. 9.2
4 Technologische Entwicklungen führen oft in einer ersten Begeisterung zu überzogenen Erwartungen am Anfang, gefolgt von Enttäuschungen, bevor es zu realistischen Anwendungen kommt.
5 „Hype Cycle für neue Technologien“ (2024) von Gartner, Inc., verfügbar unter: https://www.gartner.de
6 Vgl. 33. TB Nr. 1

nellen Lernens zur Nutzung von Gesundheitsdaten für Forschungszwecke, technologische Entwicklungen im Bereich Human Enhancement und neue Generationen von Gehirn-Computer-Schnittstellen. Diese Erkenntnisse fließen in ein Diskussionspapier zu den datenschutzrechtlichen Aspekten dieser Innovationsansätze ein, das im Jahr 2026 fertiggestellt wird.

## 2.2 Aufbau des ReguLab für mehr Rechtsklarheit und verantwortungsvolle Innovation

**Um datengestützte Innovationen bei gleichzeitiger Einhaltung eines hohen Datenschutzniveaus zu fördern, habe ich 2025 das ReguLab ins Leben gerufen.**

Das ReguLab ist ein Programm, mit dem ich die Entwicklung neuer Technologien über mehrere Monate hinweg begleiten werde. Es folgt dem Leitbild einer modernen, wirkungsbasierten Verwaltung. Mein Ziel ist die Förderung datengestützter Innovationen bei gleichzeitiger Einhaltung eines hohen Datenschutzniveaus. Grundlegend sind die Schaffung größerer Rechtsklarheit, eine einheitlichere Auslegungspraxis sowie ein konstruktiver Beitrag zur Weiterentwicklung gesetzlicher Rahmenbedingungen.

Um Rechtsklarheit für einen erfolgreichen Praxiseinsatz zu schaffen, sollen Datenschutzfragen gemeinsam mit den Innovatorinnen und Innovatoren frühzeitig gelöst werden. Datenschutz wird dadurch zum Qualitätsmerkmal, das Vertrauen in die Innovation stärkt. Das ReguLab trägt zur Rechtsklarheit bei, indem es aufzeigt, wie technologische Innovationen auch in rechtlichen Graubereichen grundrechtskonform möglich sind, es beugt Fehlentwicklungen vor und steht für eine progressive Datenschutzkultur.

Für das ReguLab habe ich mich für eine wirkungsbasierte Herangehensweise entschieden. Der Fortschritt wird auf Basis eines klar definierten Wirkmodells gemessen, in dem festgehalten wird, welche konkreten Veränderungen herbeigeführt werden sollen und welche Ressourcen und Leistungen hierzu erforderlich sind. So stellt mein Haus sicher, dass unsere Arbeit nachhaltig wirkt und Veränderungen über einzelne Bereiche hinaus anstößt. Die wesentlichen Aspekte dieses wirkungsorientierten Konzepts sind:

- Input: Meine Behörde bringt fachliche Expertise, Ressourcen und ein Netzwerk aus Expertinnen und Experten ein.
- Output: Unmittelbare Ergebnisse sind dokumentierte Lösungswege und Erkenntnispapiere.
- Outcome: Mittelfristig zielt das ReguLab darauf ab, die Anwendungskompetenz bei Innovatorinnen und Innovatoren zu steigern. Sie entwickeln ein praxisbezogenes Verständnis für Datenschutzanforderungen und integrieren diese frühzeitig („Privacy by Design“).
- Impact: Langfristig soll dies zur Stärkung einer progressiven und befähigenden Datenschutzkultur beitragen, die Grundrechtsverletzungen vorbeugt.

**Detaillierte Darstellung des Wirkmodells**

(QR-Code klicken oder scannen)

Das Programm steht grundsätzlich allen Akteurinnen und Akteuren offen, die innovative datengetriebene Technologien entwickeln oder einsetzen möchten. Dies umfasst insbesondere Bundesbehörden und öffentliche Stellen, Forschungseinrichtungen sowie Unternehmen.

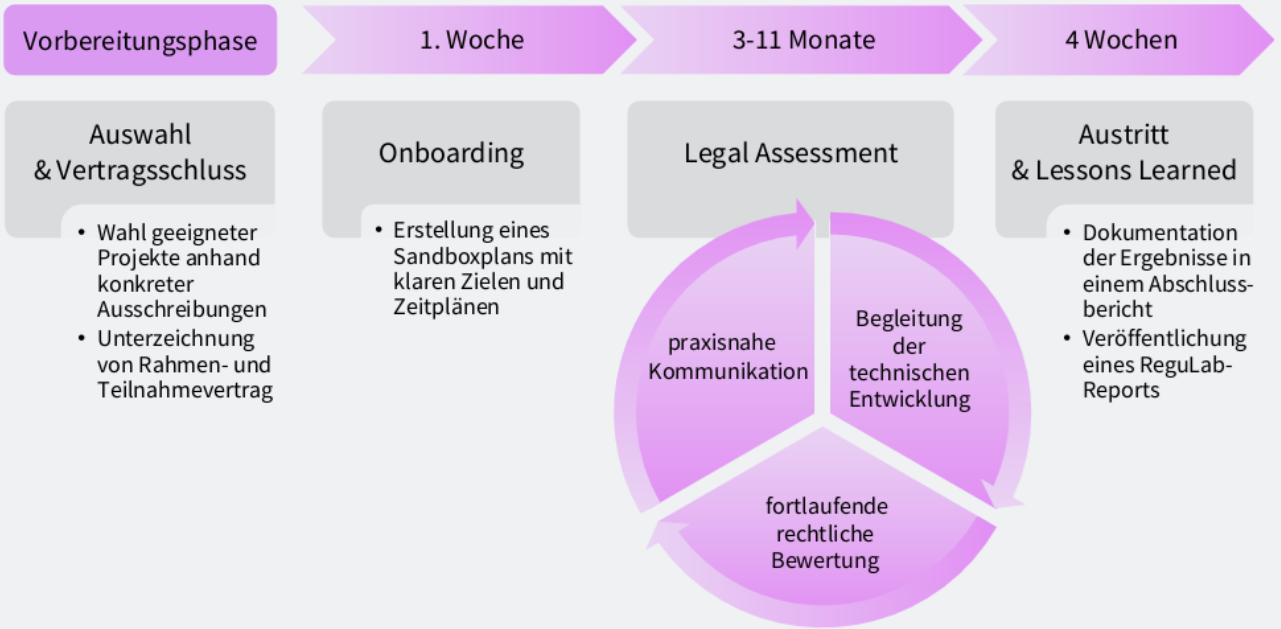
Wesentliche Voraussetzungen sind, dass die Projekte mit grundlegenden datenschutzrechtlichen Unsicherheiten konfrontiert sind und die Bereitschaft besteht, in einem definierten Rahmen kooperativ und transparent mit meiner Behörde zusammenzuarbeiten. Ein entscheidender Faktor bei der Auswahl ist die Übertragbarkeit der Projektergebnisse. Der Use Case soll für möglichst viele weitere Akteure relevant sein, da die Ergebnisse der ReguLab-Teilnahme veröffentlicht werden.

Die teilnehmenden Projekte durchlaufen vier Phasen: Nach der vorbereitenden Auswahl- und Vertragsanbahnungsphase wird in der Onboarding-Phase zunächst ein Sandboxplan mit klaren Projektzielen und Zeitplänen definiert. Hiernach beginnt die Phase des Legal Assessments: Die technische Entwicklung der Innovation wird auf Grundlage regelmäßiger Austauschformate mit den ReguLab-Teilnehmenden eng begleitet und fortlaufend

rechtlich bewertet. In der abschließenden Phase erfolgt die systematische Dokumentation der Ergebnisse. Die datenschutzrechtlichen Erkenntnisse werden in ReguLab-Reports überführt und veröffentlicht. Diese sollen auch anderen Innovatorinnen und Innovatoren als Orientierungshilfe dienen.

Alle relevanten Informationen zum ReguLab sind auf der ReguLab-Webseite zentral gebündelt.[7] Den ersten Fokus habe ich im Bereich meines Schwerpunktthemas Gesundheit gewählt und hierfür inzwischen einschlägige Innovatorinnen und Innovatoren gewonnen.

**ReguLab-Prozess**






7 www.regulab.de

# 3 Schwerpunktentwicklungen



## 3.1 Gesundheit

### 3.1.1 Öffentliche Gesundheit – aktuelle Entwicklungen

**Meine Beratungstätigkeit war auch in 2025 stark von gesundheitlichen Themen geprägt.**

Der **European Health Data Space** (EHDS) ist am 26. März 2025 in Kraft getreten.[8] Durch den EHDS sollen die Bürgerinnen und Bürger über ein digitales interoperables Format mehr Kontrolle über ihre Gesundheitsdaten erhalten. So sollen sie selbst u. a. auf Rezepte, Laborergebnisse, Entlassungsberichte sowie Impfnachweise zugreifen können. Zudem soll es für sie möglich werden, den Zugang zu ihren Daten gegenüber Leistungserbringern wie Ärzten, Krankenhäusern und Apothekern zu gewähren oder zu beschränken. Daneben sieht die zugrunde liegende EU-Verordnung zahlreiche Regelungen für eine sekundäre Nutzung der Gesundheitsdaten für Forschung, Innovation und Politikgestaltung vor.

Der EHDS enthält Öffnungsklauseln, die den Mitgliedstaaten Regelungsbereiche einräumen. Mit dem federführenden Bundesministerium für Gesundheit (BMG) stehe ich hierzu – wie bereits während der Verhandlungen – in einem engen Austausch. Ich setze mich hierbei für eine Balance zwischen dem Interesse des Gemeinwohls an der Nutzung von Gesundheitsdaten bei der Leistungserbringung als auch zu Forschungszwecken einerseits und dem Schutzinteresse des Einzelnen andererseits ein. Erste Workshops zur nationalen Umsetzung des EHDS haben unter meiner Beteiligung bereits stattgefunden und werden auch 2026 fortgesetzt.

Am 9. Oktober 2025 wurde das **Forschungsdatenzentrum Gesundheit** (FDZ Gesundheit) beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) eröffnet.[9] Es bildet nunmehr die zentrale Infrastruktur für die Bereitstellung und Nutzung von Gesundheitsdaten zu Forschungszwecken im Gesundheitswesen. Die Entwicklung und Inbetriebnahme des FDZ Gesundheit erfolgten in einem engen, kontinuierlichen und konstruktiven Austausch zwischen mir und den verantwortlichen Stellen. Im Rahmen dieser vertrauensvollen Zusammenarbeit wurden die datenschutzrechtlichen und technischen Schutzkonzepte gemeinsam erörtert, weiterentwickelt und aufeinander abgestimmt. Die Eröffnung war insgesamt ein wichtiger Schritt für das Gesundheitswesen, um digitaler, souveräner und wissensbasierter zu werden. Das FDZ Gesundheit setzt neue Maßstäbe für den datenschutzkonformen Zugang zu sensiblen Gesundheitsdaten. Insbesondere die Ausgestaltung der Pseudonymisierungsverfahren, der gesicherten Verarbeitungsumgebungen sowie die Antrags- und Freigabeprozesse wurden von mir kooperativ und lösungsorientiert begleitet. Auf diese Weise gewährleistet das FDZ Gesundheit ein hohes Datenschutzniveau und ermöglicht zugleich eine praktikable Nutzung von Gesundheitsdaten zu Forschungszwecken. Eine verantwortungsvolle Datennutzung wird mit der konsequenten Gewährleistung eines hohen Datenschutzniveaus als Grundlage vertrauenswürdiger und datenbasierter Forschung verbunden.

Im November 2025 erreichte mich der Referentenentwurf des **Medizinregistergesetzes** (MRG-E). Dieser verfolgt das Ziel, eine rechtssichere, qualitativ hochwertige und datenschutzkonforme Registerforschung zu ermöglichen und hierfür einheitliche rechtliche und technische Rahmenbedingungen zu schaffen. Der Gesetzesentwurf sieht insbesondere Erleichterungen beim Datenaustausch sowie der Datenbereitstellung für Register vor, die erfolgreich ein Qualifizierungsverfahren nach dem Medizinregistergesetz durchlaufen haben. Das BMG hat den Referentenentwurf in einem intensiven, engen und konstruktiven Austausch mit mir unter Be-

8 Vgl. 31. TB Nr. 5.1, 32. TB Nr. 3.1.1, 33. TB Nr. 3.1.3
9 Vgl. 31. TB Nr. 4.1.2, 33. TB Nr. 3.1.1

rücksichtigung der besonderen datenschutzrechtlichen Anforderungen erarbeitet und fortlaufend überarbeitet.

#### 3.1.2 Bundesweiter Rollout der ePA

**Seit dem 15. Januar 2025 wurde die elektronische Patientenakte (ePA) für alle gesetzlich Versicherten von ihren Krankenkassen angelegt, soweit Versicherte dieser nicht widersprochen haben. Bislang nutzt nur eine geringe Zahl der Versicherten ihre ePA aktiv. Dies liegt allerdings nicht an den Sicherheitsanforderungen, die die Datenschutz-Grundverordnung (DSGVO) stellt. Damit die ePA ihren Mehrwert im Rahmen der Gesundheitsversorgung entfalten kann, müssen Datenschutz sowie Datensicherheit in ihr gewährleistet werden. Auch muss das Rechtemanagement verständlich sein, damit die Versicherten eine selbstbestimmte Entscheidung über die Nutzung der eigenen ePA fällen können.**

Soweit sie dieser nicht widersprochen haben, wurde mit dem gesetzlichen Wechsel von der einwilligungsbasierten Opt-In-ePA hin zur widerspruchsbasierten Opt-Out-ePA allen gesetzlich Versicherten ab dem 15. Januar 2025 von ihren Krankenkassen eine Opt-Out-ePA angelegt. Mit der widerspruchsbasierten ePA verfolgt der Gesetzgeber das Ziel einer verbesserten Gesundheitsversorgung, insbesondere zur gezielten Unterstützung von Anamnese, Befunderhebung und Behandlung. Die Widerspruchslösung soll eine vollumfängliche, weitgehend automatisierte Befüllung der ePA mit strukturierten Daten sicherstellen. In meinen vorherigen Tätigkeitsberichten aus den Jahren 2023[10] und 2024[11] habe ich bereits sowohl über meine Beratung zum Digitalgesetz als gesetzliche Grundlage für die neu gestaltete Opt-out-ePA berichtet als auch über meine Rundschreiben, mit denen ich die unter meiner Datenschutzaufsicht stehenden Krankenkassen bei ihren Informationspflichten vor Anlage der ePA unterstützt habe. Ich bin der Ansicht, dass es verständlicher und adressatengerechter Informationen bedarf, damit die Versicherten eine selbstbestimmte Entscheidung hinsichtlich der Nutzung ihrer ePA treffen können.

Nach der Testphase in den Modellregionen erfolgte der bundesweite Rollout der neu gestalteten Opt-Out ePA im April 2025. Seit Oktober 2025 müssen die Leistungserbringer, also Praxen und Kliniken, die ePA verpflichtend nutzen. Das BfDI-Datenbarometer, das regelmäßig repräsentative Bevölkerungsumfragen zu Datenschutzthemen durchführt, zeigt, dass nur rund jede zehnte Person die ePA aktiv nutzt[12]. Dies liegt jedoch nicht an vermeintlich überzogenen Sicherheitsanforderungen beim Authentifizierungsprozess. Vielmehr ergibt das Datenbarometer, dass 42 Prozent der bislang nicht authentifizierten Versicherten aktuell schlicht keinen Bedarf für eine aktive Nutzung der ePA sehen. Knapp die Hälfte der Befragten konnte sich jedoch vorstellen, in den nächsten sechs Monaten eine Authentifizierung für die ePA zu durchlaufen und damit eine aktive Nutzung zu ermöglichen. Akzeptanz sowie Nutzung der ePA befinden sich derzeit somit in einer Entwicklungsphase, die ich weiterhin begleiten werde. Hohe Sicherheitsanforderungen stellen jedoch kein Hindernis für die Nutzung der ePA dar und sind aus Datenschutzsicht notwendig.

Die Einhaltung der Vorgaben des Art. 32 DSGVO ist bei der tatsächlichen Ausgestaltung der Authentifizierung entscheidend. Hierauf habe ich bei meinem Erfahrungsaustausch mit den betrieblichen Datenschutzbeauftragten (bDSB) der gesetzlichen Kranken- und Pflegekassen im Juni 2025 hingewiesen[13]. Aus Art. 32 DSGVO ergibt sich für die verantwortlichen Krankenkassen die Verpflichtung, den Zugriff auf Gesundheitsdaten für die Versicherten so abzusichern, dass dieser erst erfolgen kann, nachdem die Zugriffsberechtigung der zugreifenden Person durch eine Authentifizierung mit dem höchstmöglichen Sicherheitsniveau nach dem Stand der Technik verifiziert wurde[14]. Bei der Einstufung des Sicherheits- bzw. Vertrauensniveaus einer Authentifizierungslösung richte ich mich nach der Bewertung des Bundesamts für Sicherheit in der Informationstechnik (BSI). Für die Authentifizierung ohne Einsatz der elektronischen Gesundheitskarte (eGK) hat der Gesetzgeber in § 336 Abs. 2 S. 1 Nr. 2 Sozialgesetzbuch (SGB) Fünftes Buch SGB (V) zudem festgeschrieben, dass die Authentifizierung unter Anwendung eines sicheren Verfahrens zu erfolgen hat, welches „einen hohen Sicherheitsstandard gewährleistet“. Davon abweichend hat er gleichzeitig in § 336 Abs. 2 S. 2 SGB V festgelegt, dass der Versicherte nach umfas-

10 Vgl. 32. TB Nr. 3.1.3
11 Vgl. 33. TB Nr. 3.1.4
12 Vgl. Die BfDI, Datenbarometer: Elektronische Patientenakte (ePA), abrufbar unter: https://www.bfdi.bund.de/DE/BfDI/Datenbarometer/ePA/ePA_node.html
13 Bericht zum gemeinsamen Erfahrungsaustausch mit den bDSB der gesetzlichen Kranken- und Pflegekassen vom 30. Juli 2026, S. 3 ff., abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2025/Rundschreiben-Erfahrungsaustausch-Kassen.pdf?__blob=publicationFile&v=3
14 Vgl. DSK-Entschließung vom 1. September 2020, S. 2, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20200901_PDSG_Entschlie%C3%9Fung.pdf

sender Information in die Nutzung eines Authentifizierungsverfahrens einwilligen kann, das einem „anderen angemessenen Sicherheitsniveau“ entspricht. Dieses kann nach Spezifikationen der Gesellschaft für Telematik (gematik) durch Nutzung von Biometrie umgesetzt werden.

Nach Untersuchungen des BSI erreichen die Biometriefunktionen der am Markt erhältlichen mobilen Endgeräte allerdings nicht das erforderliche Vertrauensniveau „hoch“, sondern bestenfalls das Vertrauensniveau „substantiell“ (Apple FaceID), meist jedoch nur das Vertrauensniveau „normal“.[15] Folglich ist für die Einhaltung des Art. 32 DSGVO für die Krankenkassen in der Praxis entscheidend, dass sie einen Zugang zur ePA anwenden und gewährleisten, der den höchstmöglichen Sicherheitsanforderungen genügt. Ein Wechsel des Versicherten auf ein anderes Sicherheitsniveau ist unter hohem Sicherheitsniveau nach initial durchgeführter Authentifizierung zwar möglich. Allerdings bleiben die Krankenkassen verpflichtet, den Zugang mit höchstmöglichem Sicherheitsniveau „vorzuhalten“, damit den Versicherten jederzeit die Möglichkeit verbleibt, in das „hohe“ Sicherheitsniveau zurückwechseln zu können.

Mit dem Wechsel von der Opt-In- zur Opt-Out-ePA hat der Gesetzgeber auch das Rechtemanagement neu geregelt. Trotz vielfältiger Widerspruchsmöglichkeiten, die in meinem 33. Tätigkeitsbericht aufgelistet sind,[16] kann aktuell nicht mehr festgelegt werden, dass einzelne Leistungserbringer nur auf bestimmte Dokumente zugreifen dürfen. Mit der Verordnung über den Europäischen Gesundheitsdatenraum (EHDS-VO) hat der europäische Gesetzgeber jedoch das Recht auf Beschränkung des Zugangs zu personenbezogenen elektronischen Gesundheitsdaten oder Teilen davon explizit geregelt. Unmittelbare Geltung entfaltet die Normierung frühestens ab 26. März 2029. Ob und wie sie sich auf das Rechtemanagement der ePA auswirken wird, werde ich mit dem Gesetzgeber, der gematik und den Krankenkassen erörtern.

Als positive Entwicklung im Rechtemanagement bewerte ich die in den Regelungsvorschlägen zum Gesetz zur Befugniserweiterung und Entbürokratisierung in der Pflege vorgesehene Änderung des § 352 SGB V. Hiernach sollen Leistungserbringer keine Abrechnungsdaten mehr in der ePA einsehen können, die Versicherten jedoch schon. Dies trägt zum Schutz vor indirekter Offenbarung von sensiblen Informationen der Versicherten bei.

Mit der gematik befinde ich mich im Rahmen meiner Beratungstätigkeit in einem regelmäßigen Austausch zur Justierung bestehender und Erstellung neuer Spezifikationen. Sobald ich Risiken erkenne, adressiere ich diese. Gemeinsam mit dem BSI begleitete ich beispielsweise die mitigierenden Maßnahmen zu der durch den Chaos Computer Club (CCC) im Dezember 2024 aufgedeckten Sicherheitslücke. Auch auf weitere Hinweise des CCC setzte ich mich in meiner beratenden Tätigkeit für sinnvolle Anpassungen der rechtlichen Grundlagen, beispielsweise im Rahmen der elektronische Ersatzbescheinigung (eEB), sowie eine datenschutzkonforme Nutzung der ePA ein.

Zukünftig wird es immer wieder neue Entwicklungen geben, bei denen ich die gematik und die gesetzlichen Krankenkassen in meinem Zuständigkeitsbereich beratend begleite. Die im Juli 2025 veröffentlichte Version der ePA enthielt z. B. eine Datenkategorie für die datengestützte Erkennung individueller Gesundheitsrisiken im Sinne des § 25b SGB V. Deshalb habe ich die Krankenkassen im Vorfeld mit einem Rundschreiben bei der Erfüllung ihrer Informationspflichten unterstützt.[17] Dies werde ich weiterhin tun und die Bürgerinnen und Bürger informieren.

## 3.2 Künstliche Intelligenz

### 3.2.1 Nationale Durchführung KI-Verordnung

**Seit 2025 ist die KI-Verordnung teilweise in Kraft. Nun beginnt die Phase der praktischen Durchführung. Eine gute Kooperation der zuständigen Stellen schafft die Grundlage für wirksamen Grundrechtsschutz und eine erfolgreiche KI-Entwicklung.**

Nachdem im Jahr 2024 die europäische KI-Verordnung (KI-VO) in Kraft getreten ist[18], haben in 2025 deren erste Vorschriften Geltung erlangt. Sowohl die DSGVO als auch die KI-VO zielen auf einen angemessenen Ausgleich zwischen wirtschaftlicher und technischer Entwicklung einerseits sowie dem Schutz der betroffenen Personen andererseits.

Seit dem 2. Februar 2025 sind die allgemeinen Bestimmungen der KI-VO einschließlich der Vorgabe zum

15 Vgl. BSI, Bewertung von Authentisierungslösungen gemäß TR-03107 in Version 1.1.1, Gliederungspunkt 4.4.1, S. 34 f.
16 Vgl. 33. TB Nr. 3.1.4
17 Rundschreiben vom 1. April 2025, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2025/Rundschreiben-gesetzl.-Kranken-Pflegekassen.pdf?__blob=publicationFile&v=1
18 Vgl. 32. TB Nr. 3.2.1

Aufbau von KI-Kompetenz sowie die Regelung über verbotene KI-Praktiken anzuwenden. Seit dem 2. August 2025 gelten die Regelungen der KI-VO über KI-Modelle mit allgemeinem Verwendungszweck (ausgenommen die dazugehörige Sanktionsvorschrift).

Ebenfalls zum 2. August 2025 waren verschiedene Stellen zur Umsetzung der KI-VO einzurichten bzw. zu benennen, darunter die zuständigen nationalen Behörden. Die deutsche Durchführung soll durch das KI-Marktüberwachungs- und Innovationsförderungsgesetz erfolgen. In dem Gesetzesentwurf der Bundesregierung ist die Bundesnetzagentur als eine Marktüberwachungsbehörde und zentrale Anlaufstelle nach der KI-VO vorgesehen. Bestehende Zuständigkeiten der Datenschutzaufsichtsbehörden werden hierdurch nicht berührt. Als unabhängige Instanz, die mit dem Schutz der Grundrechte betraut ist, erwachsen mir als BfDI aus der KI-VO neue Befugnisse in Bezug auf die Verwendung bestimmter Hochrisiko-KI-Systeme. So können bspw. technische Tests von Hochrisiko-KI-Systemen beantragt werden, um diese datenschutzrechtlich zu überprüfen.

Viele KI-Systeme beruhen auf der Verarbeitung personenbezogener Daten. Eine enge, strukturierte Zusammenarbeit nach dem Grundsatz der loyalen Zusammenarbeit zwischen den Marktüberwachungsbehörden im Sinne der KI-VO und den Datenschutzbehörden ist nicht nur im Interesse der Effektivität der Aufsicht erforderlich. Einheitliche rechtsaktübergreifende Auslegungen und klar nachvollziehbare Zuständigkeiten schaffen Rechtssicherheit und Planungsklarheit. Diese Rechtssicherheit ist ein entscheidender Erfolgsfaktor für die Entwicklung und den Einsatz von KI mit europäischen Werten und stärkt zugleich Deutschland als attraktiven KI-Wirtschaftsstandort.

Ein Beitrag zu dieser Rechtsklarheit soll durch Leitlinien des Europäischen Datenschutzausschusses zum Zusammenspiel von KI-VO und Datenschutzbestimmungen erfolgen. Die Arbeit an den Leitlinien[19] wurde im Berichtsjahr unter Beteiligung meiner Mitarbeiterinnen und Mitarbeiter intensiv fortgesetzt und erfolgt nunmehr in Kooperation mit der Europäischen Kommission.

## 3.3 Sicherheit

### 3.3.1 Gesetzgebungsvorhaben – Polizei, Nachrichtendienste und Sicherheits- sowie Zuverlässigkeits- und Verfassungstreueprüfungen

**Auch in diesem Jahr habe ich zahlreiche Gesetzentwürfe begleitet. Ich sehe Licht und Schatten: endlich wurde z. B. die Reform des Bundespolizeigesetzes und des MAD-Gesetzes eingeleitet. Auch die Differenzierung zwischen Sicherheitsüberprüfungen einerseits und sonstigen Personenüberprüfungen andererseits finde ich grundsätzlich richtig. Nicht nur in diesen Gesetzen musste ich aber auch viele Punkte kritisch anmerken. Besonders negativ ist dabei aufgefallen, dass unter dem Stichwort Bürokratieabbau versucht wurde, den Grundrechtsschutz zu schwächen. In eigener Sache kritisiere ich weiterhin, dass mir die Zuständigkeit für die Datenschutzaufsicht über die Nachrichtendienste des Bundes genommen werden soll.**

#### Modernisierung des Bundespolizeigesetzes

Die Bundesregierung hat am 3. Dezember 2025 einen Gesetzentwurf zur Modernisierung des BPolG in den Bundestag eingebracht (BT-Drs. 21/3051).

Ich begrüße zunächst die längst überfällige Umsetzung der Richtlinie (EU) 2016/680 (JI-Richtlinie) bezogen auf wirksame Abhilfebefugnisse der Datenschutzaufsicht. Hier hatte die EU-Kommission bereits zwei Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Allerdings schränkt der BPolG-Entwurf meine Abhilfebefugnisse unangemessen ein, da er eine Pflicht zur vorherigen Beanstandung von Verstößen sowie eine zusätzliche Erheblichkeitsschwelle für weitere Maßnahmen fordert. Auch den Ausschluss von Löschanordnungen in der Gesetzesbegründung halte ich für nicht vereinbar mit dem Unionsrecht, da die Löschung in vielen Konstellationen die einzige Möglichkeit darstellt, einen Datenschutzverstoß effektiv zu beseitigen.

Aus Datenschutzsicht ist bedauerlich, dass das besonders eingriffsintensive Instrument der Quellen-Telekommunikationsüberwachung wieder Einzug in den Gesetzentwurf gefunden hat. Der Einsatz sog. **„Staatstrojaner“** birgt trotz verfahrenssichernder Maßnahmen etwa zum Kernbereichsschutz erhebliches Missbrauchspotenzial. Zudem sind Kontrollmöglichkeiten für Gerichte und Aufsichtsbehörden aufgrund der technischen Komplexität eingesetzter Software-Lösungen häufig stark eingeschränkt.

19 Vgl. 32. TB Nr. 3.2.2

Insgesamt enthält der Entwurf zahlreiche neue, teilweise eingriffsintensive Ermittlungsbefugnisse (u. a. Erhebung von Verkehrs- und Nutzungsdaten, Datenerhebung mit besonderen Mitteln wie Observationen), die an einheitliche Voraussetzzungen geknüpft werden sollten, wie etwa abschließende Straftatenkataloge mit Bezug zur Bundespolizei.

Positiv ist anzumerken, dass der Entwurf regelmäßige Pflichtkontrollen durch mein Haus im Hinblick auf heimliche und eingriffsintensive Maßnahmen sowie hiermit zusammenhängende Datenübermittlungen enthält.

**Gesetz zur Stärkung der militärischen Sicherheit in der Bundeswehr**

Mit dem Artikelgesetz zur Stärkung der Militärischen Sicherheit in der Bundeswehr[20] hat die Bundesregierung u. a. ein Gesetz über den Militärischen Abschirmdienst (MADG) vorgelegt. Dieses ist das erste der drei Nachrichtendienst-Gesetze, das die ausstehenden Änderungsforderungen des Bundesverfassungsgerichts (BVerfG)[21] umfassend angeht und aus meiner Sicht auch in weiten Teilen erfüllt. Defizite sehe ich vor allem noch in vier Bereichen:

- Eingriffsintensive nachrichtendienstliche Mittel müssen durch eine unabhängige Vorabkontrolle – hier die Richterin oder den Richter am Amtsgericht – genehmigt werden. Das Gesetz stellt dies allerdings nicht durchgängig sicher.
- Der Militärische Abschirmdienst (MAD) bekommt die Befugnis zum heimlichen Zugriff auf Informations- und Kommunikationstechnik kommerzieller Anbieter und zum Kopieren aus dieser, um einen Cyberangriff auf das Bundesministerium der Verteidigung (BMVg) oder dessen Geschäftsbereich nachzuverfolgen. Ich halte es für notwendig, dass technische Sicherheitsvorkehrungen wie Protokollierung und Löschung sowie eine Regelung zur Sicherstellung des Kernbereichsschutzes in die Vorschrift aufgenommen werden.
- Der MAD erhält zudem Befugnisse, Maßnahmen gegen Ausländerinnen und Ausländer im Ausland durchzuführen. Nach der Rechtsprechung des BVerfG dürfen Unterschiede beim nachrichtendienstlichen Handeln im Ausland zwischen Ausländerinnen und Ausländern einerseits und Deutschen andererseits zwar gemacht werden, aber Ausländerinnen und Ausländer nicht pauschal schlechter gestellt werden als Deutsche[22]. Unterschiede dürfen nach der Rechtsprechung im Ergebnis nur wegen im Ausland vorherrschender Umstände gemacht werden, die zu einer zusätzlichen Erschwerung oder Gefährdung nachrichtendienstlicher Arbeit führen. Diese Voraussetzungen erfüllt das Gesetz nicht.
- Ähnlich wie bereits das Bundesverfassungsschutzgesetz (BVerfSchG) soll auch das MADG Vorschriften enthalten, die den MAD zu diversen Eigensicherungsmaßnahmen ermächtigen[23]. Im MADG fehlen aber wichtige Aspekte zu Transparenz, Aufbewahrungs- und Löschfristen.

Von diesen Defiziten abgesehen, erachte ich das Gesetz in vielen Teilen als gelungen. Positiv habe ich zur Kenntnis genommen, dass das BMVg und im Ergebnis auch der Bundestag es als gute Lösung ansehen, dass die Datenschutzkontrolle weiterhin in meiner Zuständigkeit bleibt. Leider ist zu befürchten, dass diese Regelung nicht von Dauer ist, da Vertreter der Bundesregierung bereits angekündigt haben, hier Änderungen anzustreben.

Darüber hinaus wird in Artikel 2 des o. g. Gesetzes ein eigenes Bundeswehr-Schutz-Gesetz (BwSchutzG) geschaffen, das am 1. Juli 2026 in Kraft treten soll. Ich begrüße, dass hier passgenaue Regelungen zur Prüfung der Verfassungstreue im Einstellungsverfahren der Bundeswehr und zur intensivierten erweiterten Sicherheitsüberprüfung geschaffen wurden. Allerdings sollten die Verfassungstreueprüfungen nicht in einem gesonderten Gesetz, sondern zentral in ein überarbeitetes Sicherheitsüberprüfungsgesetz (SÜG) überführt werden. Das neue BwSchutzG führt zusammen mit weiteren Sonderregelungen hingegen zur Zersplitterung von Personen- und Sicherheitsüberprüfungen[24].

**Sicherheitsüberprüfungsgesetz**

Nachdem eine Novellierung des SÜG in der 20. Legislaturperiode nicht abgeschlossen werden konnte, wurde das Vorhaben nunmehr erneut aufgegriffen und mittler-



20 BT-Drs. 21/1846
21 Vgl. Urt. v. 26.04.2022, 1 BvR 1619/17; Beschl. v. 28.09.2022, 1 BvR 2354/13; Beschl. v. 17.07.2024, 1 BvR 2133/22
22 Vgl. Urt. v. 19.05.2020, 1 BvR 2835/17
23 Vgl. 32. TB Nr. 3.3.1
24 Siehe auch meine Stellungnahme zur SÜG-Reform, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2025/StgN_SUEG.html?nn=251880

weile abgeschlossen[25]. Insbesondere mit Blick auf eine weiter anstehende Digitalisierung war dieser Schritt lange überfällig[26]. Die Änderungen gehen aus meiner Sicht nicht weit genug und schaffen neue Abgrenzungsprobleme. Deutlich erweiterte Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sind unverhältnismäßig.

Der Gesetzgeber ist dazu übergegangen, Personenüberprüfungen in Fachgesetzen vorzusehen und nicht mehr pauschal auf das SÜG zu verweisen[27]. Aus meiner Sicht ist dies der falsche Weg. Das SÜG sollte neugefasst und sämtliche Arten von Personenüberprüfungen zusammengeführt werden. Mangels Änderung meiner Befugnisse habe ich weiterhin gegenüber Unternehmen im Bereich des SÜG keine Möglichkeit, Abhilfemaßnahmen wie Anweisungen zu erlassen oder Bußgelder zu verhängen. Hierdurch sind besonders sensible personenbezogene Daten im Anwendungsbereich des SÜG schlechter geschützt als im Anwendungsbereich der DSGVO. Daneben sehe ich u. a. folgende Änderungen kritisch:

- Durch die vollständige Gleichstellung des Sabotageschutzes werden nun wesentlich mehr Personen (Stichwort: mitbetroffene Person) geprüft, zu denen bislang gar keine oder nur wenige personenbezogene Daten verarbeitet wurden. Dies halte ich für unverhältnismäßig.
- Die deutliche Ausweitung der Internetrecherche ist in ihrer Gesamtheit bedenklich. Dies betrifft insbesondere die Einbeziehung der mitbetroffenen Person bei allen Überprüfungsarten allein aufgrund des Näheverhältnisses sowie die erweiterten Angabepflichten ohne zeitliche bzw. inhaltliche Begrenzung.
- Die neue Rechtsgrundlage zur Verarbeitung personenbezogener Daten Dritter, die nach erfolgter Prüfung überhaupt keine Rolle spielen, ist unverhältnismäßig. Dies ist mit dem Grundsatz der Datenminimierung nicht zu vereinbaren.[28]

**Reform des Nachrichtendienst-Rechts**

Bereits im 33. TB habe ich darüber berichtet, dass die Bundesregierung Überlegungen verfolgte, mir die Zuständigkeit der Datenschutzaufsicht über den Bundesnachrichtendienst (BND), das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für den Militärischen Abschirmdienst (BAMAD oder auch MAD) zu entziehen.[29] Die Bundesregierung verfolgt dieses Ziel in der 21. Wahlperiode weiterhin. Ich habe hierzu gegenüber der Bundesregierung umfangreich dargelegt, warum ich diese Zuständigkeitsverlagerung für eine kostenintensive Verschlechterung des Grundrechtsschutzes halte. Eine den gesamten Sicherheitsbereich umfassende Datenschutzkontrolle, die Nachrichtendienste, Polizeien und Strafverfolgung gleichermaßen in den Blick nimmt, ist unverzichtbar. Dies gilt vor allem für die Kompensationsfunktion, die mir verfassungsgerichtlich zugeschrieben ist, denn betroffene Personen wissen nicht notwendigerweise in diesem Kontext, dass ihre Daten verarbeitet werden. Im Rahmen der anstehenden Gesetzesreform mit einer geplanten umfassenden Ausweitung der Befugnisse für die verschiedenen Sicherheitsbehörden ist das notwendiger denn je.

Diese Bedenken bleiben bestehen und ich sorge mich auch aufgrund meiner diesjährigen Kontrollergebnisse, z. B. im Bereich des BND, darum, dass die Datenschutzkontrolle und somit der Grundrechtsschutz über die Nachrichtendienste in der anstehenden Reform zugunsten von Sicherheitsinteressen ins Hintertreffen geraten.

**Gesetz zum Bürokratierückbau**

Mit einer Frist von nur zwei Tagen wurde ich in der Ressortabstimmung zum Entwurf eines Gesetzes für den Bürokratierückbau im Bereich des Bundesministeriums des Innern[30] als Teil der Modernisierungsagenda der aktuellen Bundesregierung beteiligt.

Gegenstand des ursprünglichen Entwurfs waren zahlreiche Änderungen des Bundeskriminalamtgesetzes. Mit dem ersten Entwurf wurde u. a. geplant, meine Beteiligung in Form des „Ins-Benehmen-Setzen“ an mehreren Stellen zu streichen. Die Kontrollintervalle für die Pflichtkontrollen sollten von zwei auf drei Jahre hochgesetzt werden. Außerdem war beabsichtigt, dass mir das BKA sein Verzeichnis der Verarbeitungstätigkeiten nicht mehr vorlegen muss. Besonders relevant waren für mich die geplante Anhebung der Aussonderungsprüffristen insgesamt und die Möglichkeit, alte Speicherungen „mitzuziehen“, wenn neue Speicherungen hinzukommen. Zu der sog. Mitziehklausel habe ich mich in mehreren

25 BT-Drs. 21/1926
26 Vgl. 33. TB Nr. 5.2.1, 32. TB Nr. 3.3.5
27 Siehe voranstehende Ausführungen zum BwSchutzG.
28 Vertieftere Ausführungen unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2025/StgN_SUEG.html?nn=251880
29 Vgl. 33. TB Nr. 3.3.2
30 BR-Drs. 639/25

Gesetzentwürfen in der Vergangenheit immer wieder klar ablehnend positioniert.

Durch die Entscheidung des Bundesverfassungsgerichts vom 1. Oktober 2024[31] fühle ich mich in meiner Position bestärkt. Darin hatte das Gericht betont, dass es gesetzliche Regelungen für eine angemessene Speicherdauer geben muss, weil die Gründe der Speicherung mit der Zeit an Gewicht verlieren.[32] Die geplante Änderung als Bestandteil des „Bürokratieabbaus“ zu bezeichnen, ist meines Erachtens irreführend. Die gesetzlichen Aussonderungsprüffristen sind Schutzvorschriften für Bürgerinnen und Bürger. Sie sollen verhältnismäßiges Handeln der Behörden sicherstellen, damit zum Beispiel die Daten zu einer Person, die von einem Vorwurf freigesprochen oder bei der das Strafverfahren aus Mangel an Beweisen eingestellt wurde, nicht unnötig lange gespeichert werden. Es handelt sich somit gerade um einen Schutz vor „Bürokratie“. Dem Vorhaben, diesen Schutz unter dem Deckmantel des „Bürokratieabbaus“ deutlich abzuschwächen, bin ich entschieden entgegengetreten.

Nachdem ich mich zu dem Entwurf kritisch geäußert und verdeutlicht habe, dass durch die geplanten Änderungen der Grundrechtsschutz der Betroffenen eingeschränkt werde, hat das BMI meine wichtigsten Änderungsvorschläge umgesetzt. Es hat insbesondere die sogenannte Mitziehklausel gestrichen und davon abgesehen, meine frühzeitige Beteiligung einzuschränken.

**Insgesamt empfehle ich der Bundesregierung im Bereich der Sicherheitsgesetzgebung,**

- **→ die Anforderungen des Bundesverfassungsgerichts vollständig in den Nachrichtendienst-Gesetzen umzusetzen,**
- **→ die Zuständigkeit für die Datenschutzkontrolle über die Nachrichtendienste des Bundes bei der BfDI zu belassen,**
- **→ alle Arten von Personenüberprüfungen, die der Sicherheit der Bundesrepublik dienen, im SÜG zusammenzuführen, anstatt diverse Regelungen in den jeweiligen Fachgesetzen vorzusehen,**
- **→ die Befugnisse der BfDI im Bereich des Sicherheitsüberprüfungsgesetz sowie bei allen Arten von Personenüberprüfung an das Niveau der DSGVO und der JI-Richtlinie anzupassen,**
- **→ die Möglichkeit der Verarbeitung personenbezogener Daten Dritter, die in überhaupt keinem Zusammenhang mit der gegenständlichen Sicherheitsüberprüfung stehen, zu streichen.**

**Querverweis:**

7.6 Datenschutzkontrolle beim Bundesnachrichtendienst



31 BVerfG Urt. v. 01.10.2024, 1 BvR 1160/19

32 BVerfG Urt. v. 01.10.2024, 1 BvR 1160/19, insb. Ls. 3 b

# 4 Einzelthemen

## 4.1 Erster Dienst zur Einwilligungsverwaltung anerkannt

**Ich habe erstmalig einen Dienst zur Einwilligungsverwaltung im Internet anerkannt.**

Einwilligungsbanner sind im Internet allgegenwärtig. Sie liefern die Rechtsgrundlage für das Setzen von „Cookies“ nach § 25 Abs. 1 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG). Wer im Internet surft, wird auf Cookie-Bannern allzu oft mit so vielen Informationen überschüttet, dass der Inhalt nicht wirklich durchdrungen werden kann und die Banner schnell ungelesen „weggeklickt“ werden.

Aus datenschutzrechtlicher Perspektive ist das problematisch. Wer nicht versteht, worin er oder sie einwilligt, trifft keine informierte Entscheidung. Einwilligungsverwaltungsdienste sollen diesem Problem entgegenwirken und bei der Bündelung und dem Verständnis von Informationen helfen. Sie verwalten einmal getroffene Entscheidungen der Nutzerinnen und Nutzer und übermitteln diese im Bedarfsfall an den Anbieter von digitalen Diensten.

Seit dem 1. April 2025 ist in Deutschland die Einwilligungsverwaltungsverordnung in Kraft. Sie ermöglicht die Anerkennung dieser Dienste zur Einwilligungsverwaltung durch meine Behörde. Mit der Anerkennung bestätige ich, dass der Dienst die an ihn nach der Verordnung gestellten Anforderungen erfüllt. Insbesondere bedeutet dies, dass der Dienst nur Einwilligungen verwaltet, die von vornherein den Anforderungen an eine informierte Einwilligung entsprechen. Ich habe im Oktober 2025 erstmalig eine Anerkennung für einen „Einwilligungsmanager“ ausgesprochen.

Die EU-Kommission plant, die Einwilligung in die Online-Datennutzung über Cookie-Banner zu reformieren. Dabei sollte sie mutig sein und auf nutzerfreundliche Einwilligungsmanager zur Verwaltung von Datenschutzeinstellungen setzen.

Dies bestätigt eine Befragung des Meinungsforschungsinstituts forsa für das neue „Datenbarometer“[33] meines Hauses. Zwei Drittel der Befragten können sich die Nutzung eines solchen Managers gut vorstellen. Mehr als 70 Prozent geben an, er würde ihnen das Gefühl geben, bei der Internetnutzung mehr Kontrolle über die eigenen Daten zu erhalten.

83 Prozent der Befragten wünschen sich, dass die vorgenommenen Einstellungen auf allen Webseiten gelten. Dafür müsste der Gesetzgeber handeln und eine Pflicht für Webseiten-Betreiber vorsehen, die vom Nutzer gegenüber dem Einwilligungsmanager getätigten Einstellungen zu beachten.

## 4.2 EUDI-Wallet – nationale Umsetzung der europäischen Brieftasche für die digitale Identität

**Die reformierte eIDAS Verordnung erweitert die eID-Systeme der Mitgliedstaaten zur elektronischen Identifizierung um die elektronische Brieftasche. Damit die Brieftasche in der sehr kurzen Frist zur Bereitstellung ein Erfolg werden kann, sollte die Bundesregierung Funktionen priorisieren, die die Rechte der Bürgerinnen und Bürger schützen.**

Im März 2024 wurden Änderungen an der EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS VO) verabschiedet. Die Mitgliedsstaaten (MS) sind demnach verpflichtet, Bürgerinnen und Bürgern eine Brieftasche für die digitale Identität zur Verfügung zu stellen (EUDI-Wallet). Bisher haben die MS nur

33 https://www.bfdi.bund.de/DE/BfDI/Datenbarometer/Cookies-PIMS/Cookies-PIMS_node.html

eID-Systeme zur Verfügung gestellt: In Deutschland ist das die Onlineausweisfunktion des Personalausweises, des elektronischen Aufenthaltstitels und der eID-Karte für Bürgerinnen und Bürger aus EU-Mitgliedstaaten.

Wallets oder digitale Brieftaschen gehen einen Schritt weiter als reine eID-Systeme. Mit ihnen sollen auch Nachweise und Attribute, die über Identitätsdaten hinausgehen, vorgehalten und für Dienstleistungen im Digitalen vorgelegt werden können. Das ermöglicht, in einer App nicht nur den Ausweis, sondern auch beliebige andere Attribute, wie z. B. die Fahrerlaubnis, Zugangsberechtigungen und Zeugnisse, aber auch Mitgliedschaften oder Konzerttickets abzulegen. Diese Weiterentwicklung einer staatlich-regulierten, sicheren digitalen Identität begrüße ich, da sie als „Schlüssel" für alle digitalisierten Lebensbereiche genutzt werden kann. Wichtig ist die Wahrung der Rechte der Bürgerinnen und Bürger.

Die Frist für die MS, bereits Ende 2026 jeweils eine EUDI-Wallet anzubieten, ist sehr kurz. Wichtige technische Standards müssen noch definiert werden. Die EUDI-Wallet wird zwar angebotsseitig von vielen Digitalisierungsprojekten als Befreiungsschlag erwartet, gleichzeitig kann sie nachfrageseitig nur erfolgreich werden, wenn Bürgerinnen und Bürger Vertrauen in die Lösung haben. Dazu muss die konkrete EUDI-Wallet-Lösung ihre Rechte aus der Verordnung wirksam sichern.

Die Bundesregierung sollte die Funktionen priorisieren, die eine sichere Basis für die Nutzenden bilden. Dazu gehört insbesondere die Möglichkeit, die Wallet pseudonym nutzen zu können, wo kein Gesetz eine Identifizierung fordert. So haben Nutzende das Recht, bei allen anderen Gelegenheiten freigewählte Pseudonyme beim Namen, der Adresse und dem Geburtsdatum zu wählen – beispielsweise bei der Registrierung zu einem sozialen Netzwerk. Die Übermittlung dieser Pseudonyme muss durch die Infrastruktur der Wallet unterstützt werden. Ebenso müssen die Wallet und ihre Infrastruktur technische Pseudonyme unterstützen. Sie verhindern, dass Anmeldungen bei verschiedenen Diensten miteinander verknüpft werden können.

Registrieren müssen sich alle Stellen (Relying Parties), welche die Daten der Wallet nutzen wollen (Art. 5b Abs. 1). Dabei ist es wichtig, allen akzeptierenden Stellen eine einfache und kostengünstige Möglichkeit der Registrierung einzuräumen. Für kleinere Unternehmen gilt dies im Besonderen. Nur wenn alle akzeptierenden Stellen registriert sind, wissen Nutzende, wem sie Daten freigeben. Das wäre eine Voraussetzung für das Entstehen von Vertrauen bei den Bürgerinnen und Bürgern und für viele Stellen, die grundsätzlich bereit sind, eine Wallet zu akzeptieren.

## 4.3 Chatkontrolle

**Und täglich grüßt die Chatkontrolle: So fühlte es sich 2025 oftmals in dem nun schon seit dreieinhalb Jahren andauernden Gesetzgebungsverfahren an. In den intensiven Verhandlungsphasen gab es beinahe täglich Updates zu neuen Ansätzen der jeweiligen Ratspräsidentschaft, um eine Einigung zwischen den EU-Mitgliedstaaten herbeizuführen. Kurz vor Jahresende 2025 konnte sich der Rat der EU auf eine gemeinsame Linie einigen. Die weiteren Verhandlungen zwischen EU-Kommission, Rat der EU und Europäischem Parlament (Trilog) sind Mitte Dezember 2025 gestartet.**

Auch im Jahr 2025 habe ich mich wieder intensiv mit der sog. Chatkontrolle (dem Entwurf einer EU-Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern bzw. CSA-Verordnung) beschäftigt.

Von mir und vielen anderen Datenschutzaufsichtsbehörden und Nichtregierungsorganisationen wird eine Durchbrechung der Ende-zu-Ende-Verschlüsselung, bzw. die verpflichtende Einführung eines Scannens von Nachrichten auf dem Endgerät vor der Verschlüsselung (sog. Client-Side-Scanning) nach CSAM kritisiert. Mit der Einigung im Rat der EU ist der Erlass verpflichtender Aufdeckungsanordnungen und damit die anlasslose und massenhafte Chatkontrolle hoffentlich endgültig vom Tisch.

Mit dem nun verfolgten Ansatz ist meinem größten Kritikpunkt Rechnung getragen. Es verbleiben jedoch noch weitere kritische Punkte aus dem Entwurf einer CSA-Verordnung.

Als BfDI setze ich mich für die Wahrung der Grundrechte von deutschen Bürgerinnen und Bürgern ein und appelliere weiterhin an die Bundesregierung sowie die europäischen Ko-Gesetzgeber, folgende Punkte bei der CSA-Verordnung einzuhalten:

- Sexualisierte Gewalt an Kindern und Jugendlichen ist ein abscheuliches Verbrechen. Sie muss bekämpft werden mit wirksamen und verhältnismäßigen Maßnahmen.
- Eine Chatkontrolle – also anlasslose Massenüberwachung gleichsam aller Bürgerinnen und Bürger – wäre in einem Rechtstaat beispiellos und schießt deutlich über das legitime Ziel (Bekämpfung sexualisierter Gewalt gegen Kinder und Jugendliche) hinaus.
- Die Vertraulichkeit der Kommunikation muss geschützt bleiben. Eine Ende-zu-Ende-Verschlüsselung darf nicht gebrochen oder durch sog. Client-Side-Scanning faktisch umgangen werden. Es drohen

massive Sicherheitslücken sowie Chilling Effekte durch einen (und sei es nur gefühlten) Überwachungsdruck auf Bürgerinnen und Bürger.

- → Pauschal verpflichtende Altersprüfungen in App-Stores sind auszuschließen. Solche Methoden können nur konkret risikoangemessen und datenminimiert eingesetzt werden, was einer pauschalen Vorschaltung entgegensteht.
- → Durch die Einrichtung eines EU-Zentrums und Berichtspflichten an dieses werden Anreize für Diensteanbieter geschaffen, CSAM-Scannen als faktisch verpflichtend anzusehen und durchzuführen. Dies könnte dazu beitragen, dass Diensteanbieter ohne Rechtspflicht eingriffsintensivere Technologien entwickeln und verwenden. Die bisherige Kritik an diesen Technologien, wie bspw. Client-Side-Scanning und das Durchbrechen der Ende-zu-Ende-Verschlüsselung, bleibt bestehen. Im Gegenteil: Derart intensive Eingriffe auf freiwilliger Basis sind besonders kritisch. Nicht zuletzt besteht das Risiko von doppelten Meldestrukturen, die eine effektive Strafverfolgung behindern könnten.
- → Für das von der CSA-Verordnung vorgesehene freiwillige CSAM-Scannen als Ausnahme vom Grundsatz der Vertraulichkeit der Kommunikation fehlt es an einer datenschutzrechtlichen Rechtsgrundlage. Eine solche ist bisher nicht in den Vorschlägen enthalten, aber aus meiner Sicht zwingend erforderlich

Im Jahr 2026 werden die EU-Kommission, der Rat der EU und das Europäische Parlament gemeinsam versuchen, sich im sog. Trilog auf eine finale Version der Verordnung zu einigen. Auch hierbei werde ich als BfDI weiterhin kritisch, aber konstruktiv die Bundesregierung beraten und mich entsprechend im Europäischen Datenschutzausschuss (EDSA) einbringen.

**Querverweis:**

4.4 Social Media ab 16? Über Altersprüfungen in digitalen Diensten

## 4.4 Social Media ab 16? Über Altersprüfungen in digitalen Diensten

**Während im Jahr 2024 die Möglichkeit von Altersprüfungen in weitgreifenden Bereichen des Internets noch in der Theorie diskutiert wurde[34], war das Berichtsjahr 2025 geprägt von technischen Entwicklungen und praktischen Umsetzungen. Sowohl in Großbritannien als auch in Australien traten Gesetze in Kraft[35], durch welche insbesondere Social-Media-Plattformen zu einer Altersprüfung ihrer Nutzenden verpflichtet wurden. Ich habe mich in diesem Jahr an vielfältigen Diskussionen zur Gestaltung von Altersprüfungen in digitalen Diensten beteiligt.**

Die EU hat mit dem Digital Services Act (DSA) zunächst Altersprüfungen als ein Instrument platziert, das – dem Risiko der einzelnen Plattformen nach – angemessen eingesetzt werden kann. Politisch diskutiert wird, ob das ausreicht oder ob Social-Media-Plattformen verpflichtet werden sollen, Nutzende pauschal erst ab einem bestimmten Alter zuzulassen.

Die Altersbeschränkung selbst ist datenschutzrechtlich weniger in den Blick zu nehmen. Ob Social Media erst ab einem gewissen Alter erlaubt sein sollte, ist eine fachpolitische Frage, die interdisziplinär beantwortet werden muss. Relevant für mich und mein Haus sind die zur Durchsetzung einer Altersgrenze erforderlichen Altersprüfungssysteme. Diese können und müssen datenschutzkonform ausgestaltet werden!

Methoden der Altersprüfung verarbeiten Daten, die möglicherweise eine Identifikation der Nutzenden zur Folge haben und so die anonyme bzw. pseudonyme Nutzung des Internets gefährden können. Die Übermittlung von eindeutigen Identifikatoren ist datenschutzrechtlich kritisch zu bewerten, wenn Lösungen zur Verfügung stehen, die weniger Daten übermitteln. Wie bei der EUDI-Wallet bereits erwägt, ruft der Grundsatz der Datenminimierung daher nach Zero-Knowledge-Lösungen. Das sind Lösungen, bei denen nicht der volle Umfang beispielsweise der Ausweisdaten oder das Geburtsdatum an die verifizierenden Akteure übermittelt wird, sondern lediglich die Feststellung, dass eine Person ein bestimmtes Alter erreicht hat.



34 Vgl. 33. TB Nr. 7.3.7

35 In Großbritannien: der Online Safety Act; in Australien: die Online Safety Amendment (Social Media Minimum Age) Bill 2024

Nicht weiter verfolgt werden sollten KI-basierte Techniken der Altersverifikation, die bspw. die Übermittlung von Fotos erforderlich machen. Nach Art. 9 der DSGVO unterliegt die Verarbeitung biometrischer Daten einem höheren Rechtfertigungserfordernis.

Keinesfalls sollte undifferenziert für jedes soziale Medium in Gänze eine bestimmte Altersgrenze festgelegt werden. Wie die UN-Kinderrechtskommission zurecht anerkennt, haben Kinder und Jugendliche ein Recht auf soziale Teilhabe, verkörpert durch das Grundrecht auf Informations- und Medienfreiheit. Dies kann sich auch auf die Nutzung von sozialen Medien beziehen. Eine Altersprüfung wäre in jedem Fall dann nicht verhältnismäßig, wenn mildere Mittel existieren, um den Zweck des Schutzes von Kindern und Jugendlichen im Netz gleichermaßen zu erreichen. Mildere Mittel können zum Beispiel kinderfreundliche Voreinstellungen und Designs sein, also quasi ein „Kinderschutz by design and default“. Anwendungen, die nur die erforderlichen Daten verarbeiten und für Kinder und Erwachsene gleichermaßen geeignet sind, benötigen keine Altersprüfung.

Eine allgemeingültige Handhabung von Methoden der Altersprüfung würde der Komplexität des Themas nicht gerecht. Die Risiken von Social-Media müssen für jeden Bereich einer Plattform gesondert beurteilt werden. Im jeweiligen Einzelfall muss abgewogen werden, ob ein verhältnismäßiger und dem Risiko angemessener Einsatz von Methoden der Altersprüfung möglich ist. Der Einsatz von Altersprüfungen ist also ein Balanceakt.

Um diesen Balanceakt erfolgreich zu navigieren und die Position des Datenschutzes in diesem Spannungsfeld zu stärken, habe ich im Berichtsjahr mit meinem Haus an vielen Diskussionen über Altersprüfungen teilgenommen, u. a. mit Behörden, der Politik, Wissenschaft, Wirtschaft, Zivilgesellschaft (z. B. auf dem Chaos Communication Congress) und technischen Standardisierungsgremien wie dem World Wide Web Consortium und dem Internet Architecture Board.

Die Debatte um ein Social-Media Verbot für Kinder und Jugendliche und der Umgang mit Altersprüfungen in digitalen Diensten wird maßgeblich bestimmen, wie das Internet von morgen aussieht. Ich werde mich weiterhin für eine datenschutz- und grundrechtswahrende Entwicklung einsetzen.

**Querverweis:**

4.2 EUDI-Wallet – nationale Umsetzung der europäischen Brieftasche für die digitale Identität

## 4.5 Microsoft 365

**Kaum ein Softwareprodukt wird so flächendeckend verwendet wie Microsoft 365. Verantwortliche stehen dabei vor dem Problem, dass die Software immer wieder wegen datenschutzrechtlicher Bedenken in der Kritik steht. Zumindest für öffentliche Stellen deuten sich jetzt Wege an, gemeinsam mit Microsoft auf einen datenschutzkonformen Einsatz hinzuarbeiten.**

Die Datenschutzkonferenz (DSK) hat in einem Beschluss im November 2022 festgestellt, dass Microsoft 365 auf Grundlage des von Microsoft bereitgestellten Datenschutznachtrags (Data Processing Addendum, DPA) nicht datenschutzkonform genutzt werden kann. Dieser Beschluss basierte auf dem Bericht einer Arbeitsgruppe, die sieben gravierende Mängel am DPA festgestellt hatte.

Seitdem haben sich die Rahmenbedingungen geändert. Zum einen ist der neue Angemessenheitsbeschluss auf Basis des EU-US Data Privacy Framework in Kraft getreten. Zum anderen sichert Microsoft mit der EU Data Boundary zu, dass große Teile der Verarbeitung nun innerhalb der EU stattfinden sollen. Außerdem stellt Microsoft mittlerweile ein angepasstes DPA für die öffentliche Verwaltung zur Verfügung.

Für die Nutzung personenbezogener Daten aus der Auftragsverarbeitung für eigene Zwecke von Microsoft ist eine tragfähige Rechtsgrundlage notwendig. Die Prüfung einer solchen Rechtsgrundlage setzt Kenntnis über die Art der verarbeiteten Daten sowie den korrespondierenden konkreten Zweck der Verarbeitung voraus. Auf Grundlage des aktuellen DPA lässt sich diese Prüfung auch weiterhin nicht abschließend durchführen. Verantwortliche, die Microsoft 365 einsetzen wollen, stehen indes in der Pflicht, die datenschutzkonforme Nutzung nachzuweisen.

Das vergangene Jahr hat gezeigt, dass Microsoft zu Anpassungen bereit ist. So hat der Europäische Datenschutzbeauftragte den Einsatz von Microsoft 365 bei der EU-Kommission und anderen EU-Einrichtungen nach vertraglichen und technischen Anpassungen durch Microsoft und die EU-Kommission wieder freigegeben, nachdem er diesen vorher aufgrund datenschutzrechtlicher Mängel untersagt hatte. Ich bin optimistisch, dass auch verantwortliche Stellen in Deutschland die verbleibenden datenschutzrechtlichen Fragestellungen im Dialog mit Microsoft klären können. Dabei unterstützt mein Haus gerne.

Eine zusätzliche Chance bietet das Angebot der Firma Delos. Diese soll als rein europäische Tochter des SAP-Konzerns den Microsoft-Technologiestack für öffentliche Stellen in Deutschland unabhängig von Microsoft betreiben. Im Rahmen des Projekts MSSC prüft die Bundesverwaltung die Nutzbarkeit dieses kommerziellen Angebotes. Mein Haus begleitet das Prüfprojekt intensiv in beratender Funktion, um sicherzustellen, dass das Angebot datenschutzkonform genutzt werden kann.

# 5 Ausgewählte Gesetzgebung



## 5.1 Änderungen der DSGVO

**Die Datenschutz-Grundverordnung (DSGVO) ist zum Ende des Berichtsjahrs dieses Tätigkeitsberichts gut siebeneinhalb Jahre wirksam. Trotz zwei durchgeführter Evaluierungen durch die Europäische Kommission (EU-Kommission) sind nennenswerte Änderungen an ihr bislang ausgeblieben. Im Berichtsjahr 2025 hat die EU-Kommission nun im Rahmen ihrer Digitalstrategie mit dem sog. Digitalen Omnibus (Omnibuspaket IV) u. a. Reformvorschläge zur Änderung der DSGVO vorgelegt. Nach der Intention der EU-Kommission sollen diese zu einer Entbürokratisierung und Stärkung der Wettbewerbsfähigkeit beitragen. Das von der EU-Kommission verfolgte Ziel der Entbürokratisierung teile ich zwar, das Schutzniveau der DSGVO sollte jedoch gewahrt bleiben.**

Am 19. November 2025 stellte die EU-Kommission den sog. Digitalen Omnibus (im Folgenden Omnibus) vor, der u. a. Änderungen zur DSGVO sowie zur Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie) beinhaltet. Die bezweckte Entbürokratisierung und Stärkung der Wettbewerbsfähigkeit möchte die EU-Kommission u. a. durch Präzisierungen, Klarstellungen und Vereinfachungen sowie durch bessere Abstimmungen der unterschiedlichen Digitalrechtsakte untereinander erreichen.

Wesentliche Inhalte der von der EU-Kommission vorgeschlagenen DSGVO-Änderungen sind u. a. eine Ergänzung der Definition des für den Anwendungsbereich der DSGVO relevanten Begriffs des Personenbezugs, die Eröffnung der Möglichkeit, Anträge auf Auskunft, Berichtigung oder Löschung künftig abzulehnen, wenn sie „missbräuchlich“ sind, sowie höhere Schwellen bei Meldungen von Datenschutz-Verletzungen und Regelungen für die Verarbeitung personenbezogener Daten beim Training und Einsatz von KI.

So sehr ich das Ziel der Entbürokratisierung sowie die Vereinfachung der Anwendung der DSGVO unterstütze, habe ich grundlegende Bedenken in Bezug auf einige der vorgeschlagenen Regelungen. Das Ziel der DSGVO ist der Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten, so dass diese Personen im Fokus stehen und ihre Rechte nicht aufgeweicht werden sollten.

Für einige Vorschläge halte ich die Wahl des Gesetzgebungsverfahrens in Form eines Omnibusverfahrens für ungeeignet, denn dieses bedeutet faktisch eine verkürzte Befassung der für die Gesetzgebung zuständigen Gremien. Zentrale Fragen und weitreichende Änderungen sollten nicht ohne Gesetzesfolgenabschätzung und nur auf evidenzbasierter Grundlage sowie nach sorgfältiger Beratung erfolgen. Die Vorschläge beinhalten zum Teil mehr als nur „Klarstellungen“ oder „Vereinfachungen“, darunter durchaus komplexe materiell-rechtliche Änderungen in der DSGVO, wie z. B. die vorgeschlagene Änderung der Definition des Personenbezugs. Auch hat die EU-Kommission nicht hinreichend nachgewiesen, das verfolgte Ziel der Entbürokratisierung mit einigen Vorschlägen zu erreichen.

Ausdrücklich begrüße ich die Intention der EU-Kommission, das Zusammenspiel zwischen der DSGVO und anderen Digitalrechtsakten eindeutiger und klarstellend regeln zu wollen. Auch eine Klarstellung, für welche Zwecke und unter welchen Bedingungen in Europa KI-Training mit personenbezogenen Daten stattfinden darf bzw. verboten ist, begrüße ich. Beispielsweise sollte KI-Training zu Gemeinwohlzwecken anders behandelt werden als KI-Training zu rein kommerziellen Zwecken.

Die deutschen und europäischen Aufsichtsbehörden prüfen in der Datenschutzkonferenz (DSK) bzw. dem Europäischen Datenschutzausschuss (EDSA) die Vorschläge der EU-Kommission und begleiten das Gesetzgebungsverfahren. So hat der EDSA zusammen mit dem Europäischen Datenschutzbeauftragten (EDSB) mit der Erarbeitung einer gemeinsamen Stellungnahme zu den Vorschlägen des Omnibusses begonnen.

Die DSK hat unter meiner Beteiligung mit dem Ziel der Entbürokratisierung eigene, zielführendere und weniger

einschneidende Vorschläge zur Anpassung der DSGVO entwickelt, die teilweise auch von der EU-Kommission adressierte Vorschriften (Art. 13, Art. 22, Art. 33) betreffen.

## 5.2 Verfahrens-Verordnung für die Durchsetzung der DSGVO (VVO)

**Die Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO (VVO) wurde im November 2025 final vom Europäischen Parlament und Rat verabschiedet und trat am 2. Januar 2026 in Kraft.**[36]

Durch die VVO soll die Zusammenarbeit der Aufsichtsbehörden bei der Durchsetzung des Datenschutzes in der EU verbessert werden. Sie harmonisiert die Regelungen der nationalen Verfahrensrechtsordnungen und ist daher von erheblicher Bedeutung für eine zügigere Durchsetzung der DSGVO bei der Bearbeitung von grenzüberschreitenden Fällen.

Ich habe das Gesetzgebungsverfahren zusammen mit meinem Haus auch in diesem Berichtsjahr begleitet. Ich begrüße, dass sowohl Europäisches Parlament als auch der Rat erhebliche Verbesserungen durchsetzen konnten und dabei auch die Positionen des Europäischen Datenschutzausschusses (EDSA) und der Datenschutzkonferenz (DSK) berücksichtigt haben. Dazu gehören insbesondere die Einführung von verbindlichen Verfahrensfristen, besser aufeinander abgestimmte Regeln im Kooperationsverfahren und die Stärkung der prozessualen Position der Beschwerdeführenden.

Auch wenn die neuen Regeln der VVO erst am 2. April 2027 anwendbar sein werden, haben der EDSA und die DSK bereits jetzt begonnen, die damit einhergehenden Begleitprozesse vorzubereiten und frühzeitig umzusetzen, damit die VVO auch in der Praxis funktionieren wird. Meine Mitarbeitenden wirken in den entsprechenden Gremien mit. Die VVO wird die Rechtsdurchsetzung in grenzüberschreitenden Verfahren effektiver machen und die Verfahren für Betroffene und Datenverarbeitende beschleunigen.

## 5.3 NIS-2-Umsetzungsgesetz

**Mit dem Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungsgesetz) hat der Deutsche Bundestag viele Einrichtungen der Wirtschaft und der Bundesverwaltung zur Umsetzung von Cybersicherheitsmaßnahmen und zur Meldung von Sicherheitsvorfällen verpflichtet. Damit stärkt das Gesetz auch den Schutz personenbezogener Daten.**

Das NIS-2-Umsetzungsgesetz setzt die EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS-2-Richtlinie) in nationales Recht um. Das Gesetz ist am 6. Dezember 2025 in Kraft getreten. Sogenannte wichtige und wesentliche Einrichtungen werden u. a. zu einem umfassenden IT-Risikomanagement und zur Umsetzung von Cybersicherheitsmaßnahmen sowie zur Meldung erheblicher Sicherheitsvorfälle verpflichtet. Die zentrale Rolle für die Umsetzung kommt in vielen Bereichen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu. Cybersicherheit ist untrennbar mit Datenschutz verbunden, da eine Verletzung der IT-Sicherheit regelmäßig auch den Schutz personenbezogener Daten gefährdet. Aufgrund der Aufmerksamkeit, die die neuen gesetzlichen Pflichten auf die IT-Sicherheit lenken, wird das Gesetz zugleich zum Schutz personenbezogener Daten beitragen.

Unsicherheit von IT-Produkten ist ein wesentliches Problem der IT-Sicherheit und für den Schutz personenbezogener Daten. Oftmals fließen Daten ab, weil Kriminelle Sicherheitslücken in der Software ausnutzen können. Aus diesem Grund kommt dem Schließen dieser Lücken eine zentrale Bedeutung zu. Ich habe stets gefordert, dass das BSI den klaren gesetzlichen Auftrag zur Weitergabe von Schwachstelleninformationen an den jeweiligen Hersteller erhält, damit dieser sie schließen kann. Es freut mich, dass dies nun im NIS-2-Umsetzungsgesetz berücksichtigt wurde.

Andere meiner Anmerkungen wurden nicht aufgegriffen, obwohl diese zur Entlastung der verpflichteten Einrichtungen und zur Entbürokratisierung beigetragen hätten. So lösen IT-Sicherheitsvorfälle in der Regel mehrere gesetzliche Meldepflichten aus. Sind personenbezogene Daten betroffen, muss einerseits nach § 32 BSI-Gesetz (BSIG) an das BSI gemeldet werden und andererseits nach Art. 33 Abs. 1 DSGVO an die zuständige Datenschutzbehörde. Hier hatte ich mich im Gesetzgebungsverfahren aktiv dafür eingesetzt, das Meldeverfahren so auszugestalten, dass mit der Meldungsabgabe an das BSI auch die Meldung an die jeweils zuständige Datenschutzbehörde in vereinfachter Form ermöglicht wird. Ich



36 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, ELI: http://data.europa.eu/eli/reg/2025/2518/oj

werde weiter dafür werben, dass solche Entbürokratisierungsmöglichkeiten künftig genutzt werden.

Da sowohl die NIS-2-Richtlinie als auch das NIS-2-Umsetzungsgesetz eine Weitergabe relevanter Informationen durch das BSI an zuständige Datenschutzaufsichtsbehörden vorsehen, wird meine Behörde künftig noch enger mit dem BSI zusammenarbeiten und sich auch mit Beratungsangeboten für eine hohes Datenschutzniveau bei der Ausübung der neuen Aufsichtsaufgaben des BSI einsetzen.

## 5.4 Gesetz zur Modernisierung und Digitalisierung der Schwarzarbeitsbekämpfung (SchwarzArbMoDiG)

**Das Gesetz zur Modernisierung und Digitalisierung der Schwarzarbeitsbekämpfung (SchwarzArbMoDiG) soll die Finanzkontrolle Schwarzarbeit (FKS) in die Lage versetzen, Schwarzarbeit effektiver zu bekämpfen und damit den durch Schwarzarbeit verursachten negativen gesamtgesellschaftlichen Auswirkungen entgegenzuwirken. Das Ziel heiße ich ausdrücklich gut, wichtig ist eine grundrechtsorientierte Ausgestaltung.**

Neben der Modernisierung des Schwarzarbeitsbekämpfungsgesetzes (SchwarzArbG) nimmt das SchwarzArbMoDiG auch allgemeine gesetzliche Anpassungen im Zollwesen vor. Änderungen gab es u. a. im Bundeskriminalamtgesetz (BKAG), im Zollfahndungsdienstgesetz (ZFdG) sowie im Zollverwaltungsgesetz (ZollVG).

In das **SchwarzArbG** wurde nach meinem Hinweis die überfällige Erweiterung meiner Aufsichtsbefugnisse um ein Anordnungsrecht bei Datenschutzverstößen im Bereich der JI-Richtlinie aufgenommen. Kern der Änderungen am SchwarzArbG ist die gesetzliche Festschreibung eines risikobasierten Ansatzes bei der Schwarzarbeitsbekämpfung und die Unterstützung der FKS durch das sog. operative Informations- und Datenanalysesystem (OIDA). Mit diesem den Hauptzollämtern (HZÄ) durch die Generalzolldirektion (GZD) zur Verfügung gestellten Risikoanalysesystem werden der FKS zukünftig Risikohinweise zugespielt, die sie im Rahmen ihrer Prüfungsauswahl berücksichtigen kann. Die aufgrund der Risikohinweise eingeleiteten Verfahren und sich daran anschließenden Ermittlungen können tief in die Rechte der Prüfbeteiligten und ihrer Arbeitnehmerinnen und Arbeitnehmer eingreifen. Die Datenverarbeitung findet zudem gewissermaßen „im Hintergrund“ statt und wird betroffenen Personen nicht offenbart, so dass bei einer verfassungsrechtlichen Betrachtung mangels ausreichender gerichtlicher Kontrolle ein hinreichendes Kontrollniveau auf andere Weise sicherzustellen war. Es ist daher ein wichtiger Erfolg meiner Beratung im Gesetzgebungsprozess, dass ich bei der Festlegung der Risikoindikatoren und Risikoparameter von OIDA ins Einvernehmen zu setzen bin.

Der Umfang der verarbeiteten Daten ist aufgrund der Natur der Sache groß und umfasst u. a. Daten der Landesfinanzbehörden, der Datenstelle der Rentenversicherung sowie Meldedaten der Zollverwaltung. Ich werde den Vollzug des SchwarzArbG eng begleiten und insbesondere ein Augenmerk auf die Erforderlichkeit dieser Datenverarbeitung und die Vermeidung automatisierter Entscheidungen gemäß Art. 22 DSGVO legen.

Im **ZFdG** und **ZollVG** werden Regelungen für ein Risikoanalysesystem geschaffen, das der Zollverwaltung (mit Ausnahme der FKS) durch das Zollkriminalamt (ZKA) bereitgestellt wird. Trotzdem ich bei der Festlegung von Kriterien, Kategorien und Quellsystemen für die zu verarbeitenden Daten sowie den Bewertungsmethoden anzuhören bin, habe ich aus systematischen Gründen die Aufnahme einer Einvernehmensregelung wie im SchwarzArbG für erforderlich gehalten. Das spezifische Eingriffsgewicht des Risikoanalysesystems hätte durch eine präventive, strukturell stärker abgesicherte Abstimmung mit mir als Datenschutzaufsichtsbehörde stärker ausgeglichen werden können.

Die Änderungen am **BKAG** führen dazu, dass die HZÄ etwa beim Vorgehen gegen Steuerstraftaten oder gegen Schwarzarbeit und illegale Beschäftigung unter bestimmten Voraussetzungen in den polizeilichen Informationsverbund aufgenommen werden. Eine weitere Tatbestandsalternative ermöglicht den Zollbehörden die Teilnahme am polizeilichen Informationsverbund bei der Erfüllung sehr weit formulierter Sicherungsaufgaben. Darunter lassen sich nahezu alle Bereiche der Zollverwaltung fassen, der damit gleichsam unbeschränkt Zugriff auf den polizeilichen Informationsverbund gewährt wird. Meinem Hinweis im Gesetzgebungsverfahren, die Vorschrift konkreter zu fassen, wurde nicht gefolgt. Ich werde die Umsetzung dieser Änderung eng begleiten.

# 6 Beratungsschwerpunkte



## Key Figures – Beratungen

Beratungs- und Informationsbesuche: 183
(+ 22 % zum Vorjahr)

Allgemeine Anfragen: 6330
(+ 21,15 % zum Vorjahr)

Telefonische Beratungen: 3091
(– 40,80 % zum Vorjahr)

## 6.1 Teilautomatisierte Webseitenprüfung – BfDI geht neue Wege in der Beratung

**Der Einsatz von Werkzeugen zur teilautomatisierten Webseitenprüfung eröffnet effiziente Beratungsmöglichkeiten bei digitalen Diensten.**

Die von mir beaufsichtigten Stellen betreiben eine Vielzahl von Webseiten. Bisher erfolgten Prüfungen zur Einhaltung der rechtlichen Anforderungen an diese größtenteils manuell. Die manuelle Prüfung einer Webseite verlangt erheblichen Zeit- und Personaleinsatz, wodurch der Umfang der durchführbaren Prüfungen deutlich eingeschränkt ist.

Mein Haus hat Werkzeuge entwickelt, die die manuelle Prüfung durch teilautomatisiert generierte Erkenntnisse ergänzen und ersetzen. Auf Basis des vom europäischen Datenschutzbeauftragten entwickelten Werkzeugs „Website Evidence Collector“[37] können mittels der BfDI-Werkzeuge skalierbar eine Vielzahl an Webseiten analysiert werden. Die erkannten technischen Sachverhalte (z. B. Server-Anfragen, gesetzte Cookies) werden automatisiert nach Indikatoren für die Einbindung vordefinierter Drittdienste gefiltert und sachverhaltsbezogene Prüfergebnisschreiben aus Vorlagen generiert. In diesen wird auf die gefundenen Sachverhalte, die entsprechende datenschutzrechtliche Einschätzung meines Hauses sowie konkrete gesetzeskonforme Lösungen hingewiesen.

Einen ersten Einsatz der teilautomatisierten Webseitenprüfung hat mein Haus im Berichtsjahr durchgeführt. Dabei wurden knapp 200 Webseiten des Bundes mit über 500.000 Unterseiten analysiert und die Ergebnisse auf Indikatoren zur Einbindung von Videos der Plattform YouTube geprüft. Durch diese Einbindungen werden Daten der Endgeräte der Nutzenden ohne vorher eingeholte Einwilligung an den Drittdienst übermittelt, so dass der Verdacht auf einen Verstoß gegen § 25 TDDDG besteht. Auf 38 Webseiten konnten dabei solche Indikatoren gefunden werden, so dass im Anschluss 38 Informations- und Beratungsschreiben an die jeweiligen Stellen versandt wurden. Meine Mitarbeiterinnen und Mitarbeiter standen zur Beantwortung von Fragen sowie beratend bei eigenständigen Prüfungen und der Umsetzung von Lösungen zur Verfügung. Eine Nachprüfung nach 20 Wochen ergab, dass bei ca. 60 Prozent der angeschriebenen Stellen die Webseiten angepasst und keine Indikatoren für eine Einbindung von YouTube mehr erkannt wurden.

Eine solche Anzahl an einzelnen Webseitenprüfungen und die sich daran anschließenden Beratungsleistungen hätten ohne Automatisierungskomponenten im gleichen Zeitraum nicht umgesetzt werden können. Der Ansatz der teilautomatisierten Prüfung mit anschließendem Informationsschreiben und Beratungsangebot hat sich daher als erfolgreich erwiesen, um die beaufsichtigten Stellen zu konkreten Sachverhalten gezielt zu beraten.

37 https://code.europa.eu/EDPS/website-evidence-collector

## 6.2 Rechtssicherheit im KI-Bereich durch Aufsichtspraxis und Dialog

**Mein Haus begleitet die Entwicklung und den Einsatz von Künstlicher Intelligenz (KI) aktiv. Durch Konsultationsverfahren, praxisnahe Orientierungshilfen und den kontinuierlichen Dialog mit relevanten Akteurinnen und Akteuren trägt meine Behörde dazu bei, bestehende rechtliche Spielräume zu klären und Verantwortliche bei der datenschutzkonformen Umsetzung von KI zu unterstützen. Damit der Datenschutz in der Bundesverwaltung von Anfang an berücksichtigt wird, habe ich eine „Handreichung für die Bundesverwaltung zum datenschutzkonformen Umgang mit KI“ veröffentlicht.**

Die rasante Entwicklung von KI macht deutlich, dass im KI-Bereich ein erheblicher Bedarf an Rechtssicherheit besteht. Der Gesetzgeber ist gefordert, durch die Schaffung spezifischer Rechtsgrundlagen den Rahmen des datenschutzrechtlich Zulässigen klar zu definieren. Bis zu einer solchen gesetzlichen Konkretisierung kommt der Datenschutzaufsicht die wichtige Rolle zu, durch Auslegung des geltenden Rechts Orientierung für die Praxis zu geben.

Im Berichtsjahr standen z. B. folgende Aspekte im Fokus meiner Arbeit: Die Frage nach passenden Rechtsgrundlagen, da bestehende Rechtsgrundlagen vielfach nicht auf die spezifischen Funktionsweisen von KI-Systemen ausgelegt sind. Oder die Ausübung der Betroffenenrechte, die im Kontext des KI-Einsatzes im Lichte neuer technischer Abläufe untersucht werden muss. Auch der datenschutzrechtliche Verantwortlichkeitsbegriff muss dahingehend neu beleuchtet werden. Und nicht zuletzt müssen wir betrachten, was die geltenden Datenschutz-Grundsätze für einen Einfluss auf den KI-Einsatz haben, um einen effektiven Grundrechtsschutz garantieren zu können.

Im Berichtsjahr habe ich mich intensiv mit dem Thema „memorisierte Daten“ in großen Sprachmodellen befasst. Im Mittelpunkt standen dabei Fragen zur datenschutzrechtlichen Einordnung solcher Daten, zu Risiken unbeabsichtigter Speicherung personenbezogener Informationen, zu Lösch- und Berichtigungsmöglichkeiten sowie zu technischen und organisatorischen Maßnahmen zur Risikominimierung. Zur systematischen Aufarbeitung dieser Fragestellungen führte ich im Zeitraum vom 10. Juli bis zum 31. August 2025 ein Konsultationsverfahren[38] zum datenschutzkonformen Umgang mit personenbezogenen Daten in KI-Modellen durch. Mit der Konsultation habe ich konkrete praktische Erfahrungen, technische Einschätzungen und normative Überlegungen von Akteurinnen und Akteuren aus verschiedenen Bereichen eingeholt. Gegenstand waren sieben Fragen zum Umgang mit personenbezogenen Daten in KI-Modellen, u. a. zu dem Personenbezug von großen Sprachmodellen und zu der Durchsetzung von Betroffenenrechten.

Das Interesse an der Konsultation war groß. Neben der Möglichkeit zur schriftlichen Stellungnahme habe ich einen Runden Tisch zum gemeinsamen Erfahrungsaustausch ausgerichtet. 30 Stellungnahmen aus Wissenschaft, Wirtschaft, Zivilgesellschaft und Praxis wurden durch mein Haus ausgewertet. Die gewonnenen Erkenntnisse sind Grundlage für meine weiteren Überlegungen zu einem datenschutzkonformen Umgang mit memorisierten Daten.

Darüber hinaus erarbeitete mein Haus im Berichtsjahr eine Handreichung für die Bundesverwaltung zum datenschutzkonformen Umgang mit KI.

**Handreichung der BfDI für die Bundesverwaltung „KI in Behörden – Datenschutz von Anfang an mitdenken“**

(QR-Code klicken oder scannen)

Die Handreichung gibt Behörden Orientierung und dient dazu, KI-Systeme, die auf großen Sprachmodellen beruhen (z. B. Chatbots), datenschutzkonform einzusetzen. Kernaspekte des Datenschutzes werden näher ausgeführt, insbesondere Personenbezug, Verantwortlichkeit, Rechtsgrundlagen, Betroffenenrechte und Umgang mit besonderen Kategorien personenbezogener Daten. Die Handreichung hilft dabei, den Datenschutz von Anfang an mitzudenken – dies ist mein Appell an alle Verantwortlichen. Denn Datenschutz ist ein integraler Bestandteil nachhaltiger und vertrauenswürdiger Innovation.

## 6.3 Digitaler Euro

**Der digitale Euro ist als Ergänzung zum Bargeld gedacht und soll künftig digitale Bargeld-, Karten- und Online-**

38 https://www.bfdi.bund.de/DE/BfDI/Konsultationsverfahren/KI-Modelle-pbD/KI-Modelle-pbD_node.html

**Zahlungen per Zentralbankgeld ermöglichen. Diesen Prozess begleitet mein Haus auf europäischer Ebene.**

Umgesetzt wird der digitale Euro durch das Eurosystem, das aus den nationalen Zentralbanken der Staaten der Eurozone und der Europäischen Zentralbank (EZB) besteht. Seit der Veröffentlichung des Berichts der EZB zu einem digitalen Euro im Oktober 2020 wurden wichtige Entwicklungsphasen durchlaufen. So wurde im Oktober 2025 die sog. Vorbereitungsphase abgeschlossen, die insbesondere zum Ziel hatte, einen Entwurf für das konstituierende technische Regelwerk für den digitalen Euro zu entwickeln und Anbieter auszuwählen, die bei der technischen Umsetzung des digitalen Euros unterstützen. Bereits angelaufen ist die nächste Phase, bei der es u. a. um die Festsetzung der rechtlichen und technischen Ausgestaltung geht.[39]

Mein Haus begleitet den Prozess aktiv im Europäischen Datenschutzausschuss (EDSA) und hat im Berichtsjahr ein Gutachten[40] des Support Pool of Experts des EDSA zur Frage begleitet, wie eine Offlinemodalität zur digitalen Bargeldzahlung datenschutzgemäß umgesetzt werden kann.

Des Weiteren berät mein Haus die Bundesbank, die gemeinsam mit anderen europäischen Notenbanken eine technische Kernkomponente für den digitalen Euro bereitstellen soll. Im Rahmen dieser Beratung konnte mein Haus Anfang November 2025 auf einer Verbraucherkonferenz der Bundesbank darstellen, welche Punkte essentiell beachtet werden müssen, um den digitalen Euro als ein datenschutzfreundliches Zahlungsmittel zu gestalten. Das ist zum einen eine Offline-Modalität, die ein Bezahlen mit digitalem Bargeld ohne Austausch von identifizierenden Daten ermöglicht. Zum anderen sollte bei der geplanten Online-Modalität, also der kreditkartenähnlichen Bezahlmöglichkeit für Zahlungen im Internet, ein Schwellenwert vorgesehen werden, unter dem Zahlungen auch ohne vollständige geldwäscherechtliche Überprüfung durchgeführt werden können.

Erfreulicherweise haben die Bundesbank und das Eurosystem den Datenschutz als zentrales Element für den Erfolg des digitalen Euros identifiziert, der dieses Zahlungsmittel von den bisher vorhandenen digitalen Zahlungsmöglichkeiten unterscheidet. Beide tauschen sich eng mit Datenschutzaufsichtsbehörden aus und zeigen sich offen für deren Anregungen. Ich werde das Projekt auch zukünftig eng begleiten und auf eine datenschutzfreundliche Ausgestaltung des digitalen Euros hinwirken.

## 6.4 Erfolgreiche Beratung der Bundesagentur für Arbeit

**Auch im Jahr 2025 war einer meiner Tätigkeitsschwerpunkte die Beratung der Bundesagentur für Arbeit (BA) als größte Bundesbehörde.**

Die BA als Vorreiterin der öffentlichen Hand für Digitalisierung und Automatisierung bietet bereits mehr als 50 ihrer Leistungen für Bürgerinnen und Bürger digital an. Mein Beratungsschwerpunkt im Berichtsjahr lag auf dem Einsatz von KI-Anwendungen und Cloud-Lösungen. Im konstruktiven Austausch mit der BA, u. a. auf Basis des DSK-Papiers zu Kriterien für Souveräne Clouds[41], konnten datenschutzfreundliche Gestaltungsmöglichkeiten aufgezeigt und realisiert werden, wie beispielsweise:

- Bei der Einführung einer Cloud-Anwendung konnte erreicht werden, dass die Datenverarbeitung ausschließlich im Europäischen Wirtschaftsraum (EWR) und in der Schweiz stattfindet.
- Durch den Ausschluss von sog. Hyperscalern als Unterauftragsverarbeiter kann der potenziellen Situation begegnet werden, dass trotz Zusicherung des Cloud-Anbieters für eine Verarbeitung im EWR Sicherheitsbehörden aus Drittstaaten die Herausgabe von Daten erreichen können. Bei Hyperscalern handelt es sich in aller Regel um Unternehmen aus Drittstaaten.
- Unter den zahlreichen KI-Projekten der BA haben meine Mitarbeiterinnen und Mitarbeiter insbesondere ein Large Language Model umfangreich geprüft, das bei der Erstellung von Antwortschreiben auf allgemein gehaltene Anfragen von Bürgerinnen und Bürgern unterstützen kann. Wichtige Themen waren hier die Rechtsgrundlage für die Nutzung von Daten für das Training der KI sowie die Anonymisierung und Pseudonymisierung von Daten.

39 Weitere Informationen zum Stand des Projektes sind abrufbar auf der Webseite der EZB unter: https://www.ecb.europa.eu/euro/digital_euro/progress/html/index.de.html

40 Die Veröffentlichung des Gutachtens von Prof. Dr.-Ing. Tibor Jager zur Offline-Modalität des digitalen Euro vom 20. Oktober 2025 ist in englischer Sprache abrufbar auf der Webseite des EDSA: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/digital-euro-and-its-token-based-offline_de

41 https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf sowie 32. TB Nr. 4.1.2

Ausblick: Die BA beabsichtigt als erste Pilotkundin der Delos Cloud die Nutzbarkeit dieses Angebots zu prüfen. Auch mein Haus begleitet das Prüfprojekt MSSC, das die Nutzbarkeit der Delos-Cloud für die Bundesverwaltung beinhaltet, beratend von Anfang an.

**Querverweis:**

4.5 Microsoft 365

## 6.5 Beratungs- und Kontrollpraxis im Telekommunikationsbereich

**Die BfDI bietet der Branche proaktive Beratung bei neuen Produkten oder vertraglichen Anpassungen an.**

Telekommunikationsanbieter arbeiten regelmäßig an neuen Produkten oder optimieren ihre Datenverarbeitungsprozesse. Dabei sind neben den Anforderungen der DSGVO regelmäßig auch Sonderrechtsvorgaben zu berücksichtigen (insbes. aus dem Telekommunikationsgesetz und dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz). In der konkreten Umsetzung stellen sich oft technische und rechtliche Detailfragen, die von Anbietern allein mit dem Gesetzestext nicht eindeutig zu beantworten sind.

Eine praktische Schwierigkeit kann z. B. darin bestehen, Endnutzenden Informationen zur Datenverarbeitung vollständig zur Verfügung zu stellen und diese so übersichtlich und allgemeinverständlich zu gestalten, dass Endnutzende diese realistischer Weise auch wahrnehmen. Hier herrscht bei Unternehmen oft Rechtsunsicherheit, welcher „goldene Mittelweg“ beide Maßgaben vereint.

In der Beratung können meine Mitarbeiterinnen und Mitarbeiter Entwürfe prüfen und eine verbindliche Rückmeldung geben. Das Unternehmen erhält so Rechtssicherheit und spätere Korrekturen werden vermieden. Zudem kann das Unternehmen bei Kundenbeschwerden auf das Beratungsergebnis verweisen.

Regelmäßig fließen die Ergebnisse meiner unterschiedlichen Beratungen und Kontrollen in Handreichungen[42] ein und kommen so der gesamten Branche sowie Bürgerinnen und Bürgern zugute. Meine Erwartungshaltung wird so zudem für alle Unternehmen transparent und kann frühzeitig berücksichtigt werden. Dies bedeutet aber auch, dass ich von meinen Abhilfebefugnissen und Sanktionsmöglichkeiten durchgreifend Gebrauch mache, wenn diese transparenten Maßgaben nicht beachtet oder bewusst ignoriert werden.

Im Berichtsjahr sind meinen Mitarbeiterinnen und Mitarbeitern bei mehreren Kontrollen Unternehmen aufgefallen, bei denen die Löschung von personenbezogenen Daten nicht ordnungsgemäß durchgeführt wurde. So war etwa bei einzelnen kleineren Anbietern die Löschung von Bestandsdaten nicht korrekt angelegt, die Speicherung von Einzelverbindungsnachweisen erfolgte zusammen mit den Rechnungen für zehn Jahre oder die Speicherung von Verkehrsdaten erfolgte unabhängig von der Abrechnungsrelevanz für mehrere Monate – und damit zu lange. Bei einem größeren Anbieter war zwar die Speicherung von Bestandsdaten grundsätzlich richtig umgesetzt, allerdings wurden im Detail auch hier diverse kleinere Probleme mit der Löschung festgestellt. Dies zeigt, wie sinnvoll regelmäßige Kontrollen bei den Unternehmen sind.

## 6.6 Registermodernisierung

**Die Registermodernisierung und die damit verbundenen Vorhaben betreten eine neue Phase der Umsetzung, an der ich weiterhin intensiv beratend mitarbeite. In der praktischen Umsetzung wird deutlich, dass die zugrundeliegenden Rechtsnormen punktuell angepasst werden sollten.**

Wie bereits in den vergangenen Jahren[43] habe ich im Berichtsjahr die Themen Registermodernisierung, Identifikationsnummer (IDNr) und Nationales Once-Only-Technical-System (NOOTS) begleitet. Mit dem im Dezember 2025 auch vom Bund ratifizierten Staatsvertrag NOOTS begann die Umsetzungsphase unter Leitung einer Steuerungsgruppe aus Bund und Ländern, an der ich weiter beratend beteiligt sein werde.

Im Berichtsjahr untersuchte mein Haus u. a. die sog. Vermittlungsstelle (VS). Aufgabe der VS ist die Durchführung einer abstrakten Übermittlungsberechtigungsprüfung, sobald zwei Behörden über das NOOTS Daten austauschen wollen.

Es zeigt sich, dass die jetzige Rechtslage in § 7 IDNrG nur bedingt für die geplanten digitalen Prozesse tauglich ist. Hier sollte der Bund (z. B. im Rahmen des vom BMDS bereitgestellten Digitalchecks) digitaltaugliches Recht schaffen, damit datenschutzrechtlich angezeigte techni-



42 Siehe unter: https://www.bfdi.bund.de/DE/Fachthemen/Themen-Positionen/Telekommunikation/Telekommunikation_node.html oder auch: https://www.bfdi.bund.de/DE/Buerger/Inhalte/Telefon-Internet/TelekommunikationAllg/FAQ_TK

43 Vgl. 33. TB Nr. 7.2.1, 32. TB Nr. 8.2

sche Maßnahmen wie die Übermittlungsberechtigungsprüfung nicht teilweise ins Leere laufen.

Im Rahmen meiner Untersuchung der VS fiel auch auf, dass die unterschiedlichen Rechtsgrundlagen und Systeme teilweise auseinanderlaufen. Dies liegt vor allem daran, dass das NOOTS erst nach Verabschiedung des IDNrG entwickelt wurde, so dass nunmehr erheblicher Anpassungsbedarf entstanden ist:

Die verschiedenen für die Verwaltungsdigitalisierung relevanten Rechtsgrundlagen (Onlinezugangsgesetz, IDNrG und § 139b Abgabenordnung) sollten aufeinander abgestimmt werden. Das NOOTS mit seinen datenschutzfreundlichen Elementen sollte dabei für alle Nutzungen der IDNr führend sein. Die leider weiterhin stockende Entwicklung der Bestandsdatenanzeige im Datenschutzcockpit ließe sich in diesem System effektiver realisieren.

Dieser Reformprozess sollte eine klare Trennung zwischen Steueridentifikationsnummer (Steuer-ID) und IDNr umfassen. Die teilweise zugelassene außersteuerliche Verwendung der Steuer-ID für Zwecke der Zuordnung ist systemwidrig und birgt verfassungsrechtliche Risiken, da einerseits der rein steuerliche Zweck verlassen wird, andererseits aber auch die Sicherungen des IDNrG nicht etabliert werden. Der Zweck der eindeutigen Zuordnung von Personen außerhalb des Steuerbereichs obliegt nach der Schaffung der IDNr als bereichsübergreifendem Kennzeichen alleine der IDNr nach dem IDNrG. Die unklare Trennung ermöglicht vermeidbare Rechtsverstöße, die ich im Rahmen datenschutzrechtlicher Prüfungen in der Praxis bereits feststellen musste. Im Rahmen meiner beratenden Tätigkeit erstellt mein Haus zu dieser Problematik ein Hintergrund- und Zukunftspapier, das diese Aspekte und mögliche Lösungen näher beleuchten wird.

## 6.7 Polizei 20/20 (P20)

**Das bundesweite Modernisierungsprogramm P20 bleibt auch weiterhin ein sicherheits- und datenschutzpolitisch hochrelevantes Großvorhaben. P20 kann erfolgreich sein, wenn datenschutz- und verfassungsrechtliche Vorgaben eingehalten werden.**

**Datenhaus**

Regelmäßig berichte ich über das Projekt P20 der Polizeibehörden des Bundes und der Länder.[44] Das gemeinsame Datenhaus, in dem zukünftig alle Polizeidaten getrennt nach Mandaten gespeichert werden sollen, ist Kern des Projekts. Ich begrüße, dass für dessen Funktionalitäten Open-Source-Produkte verwendet werden sollen. Diese Technologien sind technisch anpassbar und können daher auf (zukünftige) polizeifachliche und datenschutzrechtliche Anforderungen gezielt reagieren. Zusätzlich stärken sie die digitale Souveränität. Das Datenhaus steht aktuell technisch in den Startlöchern. Eine klare gesetzliche Regelung fehlt allerdings nach wie vor und ich werte es als unnötiges rechtliches Risiko, das Datenhaus nur auf Grundlage einer Auftragsverarbeitung zu betreiben.

Die technische Struktur des Datenhauses sieht für jede teilnehmende Polizeibehörde eine sog. Primärdatenbank vor, in der Daten bearbeitet und gelöscht werden können. Wenn die rechtlichen Vorschriften es zulassen, dann können auf einer Sekundärebene die Daten zum Abruf für andere Polizeibehörden zur Verfügung gestellt werden.

**Funktionalitäten**

Für die Abrufe auf der Sekundärebene soll eine sog. Kontextualisierung genutzt werden, um die Mandantentrennung in bestimmten Fällen zu durchbrechen.[45] Mit dieser Funktion sollen zum Beispiel Daten zu einem bestimmten Phänomenbereich bundesweit übergreifend freigegeben werden.

Ich halte es für möglich, den gesetzlich geregelten Informationsverbund, der den automatisierten bundesweiten Datenaustausch ermöglicht, mit der Kontextualisierung abzubilden. Wichtig ist, dass die datenschutz- und verfassungsrechtlichen Vorgaben beachtet werden. Konkret bedeutet dies, dass die Daten eine bestimmte Speicherschwelle erreicht haben müssen, die einen bundesweiten Datenaustausch rechtfertigt. Das ist die sog. Verbundrelevanz. Es handelt sich dabei um Speicherungen, die z. B. eine länderübergreifende Bedeutung oder einen internationalen Bezug haben.

Zudem muss eine negative Prognose zu der betroffenen Person erstellt worden sein. Zu den Anforderungen an die Negativprognose hat das Bundesverfassungsgericht mit seinem Urteil vom 1. Oktober 2024 eine wichtige

44 Vgl. 33. TB Nr. 7.4.4
45 Vgl. 33. TB Nr. 7.4.4

Entscheidung getroffen.[46] Es wird darauf ankommen, die Fälle herauszuarbeiten, in denen eine Kontextualisierung technisch und rechtssicher möglich ist. Anderenfalls besteht die Möglichkeit, dass Speicherschwellen unterlaufen werden. Ich befinde mich mit dem BMI hierzu aktuell in einem Beratungsprozess.

Auch weitere Funktionalitäten des Datenhauses haben in diesem Jahr an Bedeutung gewonnen. Hier möchte ich besonders die P20-Such-App erwähnen. Mit der Such-App sollen Abfragen von Bestandssystemen ermöglicht werden. Die Version 1.5, durch die der Zugriff auf die Systeme des Kraftfahrtbundesamtes ermöglicht wird, wurde mir im Berichtsjahr vorgestellt. Mit der Version 3.0 sollen weitere Datenbanken angebunden werden (z. B. das Ausländerzentralregister und das polizeiliche Informationssystem – INPOL). Es muss technisch sichergestellt sein, dass parallele Abfragen mehrerer Dateien mit einem konsolidierten Ergebnis nur dann möglich sind, wenn erstens die rechtlichen Grundlagen dies zulassen und zweitens Mitarbeiterinnen und Mitarbeiter der Polizei entsprechend ihrer Berechtigung verfahren. Mit der Such-App sind gleichzeitig auch der Basisdienst Protokollierung sowie das Identity- und Access-Management in den Wirkbetrieb gegangen. Nach meiner Einschätzung beabsichtigen die Projektverantwortlichen, eine Vollprotokollierung sämtlicher Datenverarbeitungsvorgänge vorzunehmen. Der begonnene Beratungsprozess im Berichtsjahr läuft in 2026 weiter, um Detailfragen zu klären.

Das BMI und ich stimmen überein, dass der Grundsatz der Zwecktrennung in P20 übergreifend einzuhalten ist. Es muss stets erkennbar sein, zu welchem Zweck die Polizei ein bestimmtes Datum verarbeitet. Die Polizeigesetze des Bundes und der Länder sehen übereinstimmend folgende grundlegende Zweckbestimmungen vor: Aufgabenerfüllung, Vorgangsverwaltung und Dokumentation sowie die Gefahren- und Strafverfolgungsvorsorge.[47] Das Bundesverfassungsgericht hat mit seiner Entscheidung vom 1. Oktober 2024[48] diese polizeilichen Verarbeitungszwecke und meine langjährige Prüfpraxis bestätigt. In der Praxis wird es darauf ankommen, ob dem Grundsatz ausreichend Rechnung getragen wird.

Der Beratungsprozess im BMI und die Beteiligung als solche verläuft äußert konstruktiv und ich werde weiterhin regelmäßig beteiligt. In diesem Berichtsjahr hat das erste Mal eine gemeinsame Informationsveranstaltung des BMI und mir stattgefunden, um den parlamentarischen Raum über P20 zu informieren.[49]

## 6.8 Beratung BfJ zu ausländischen Strafregisterauskünften

**Seit 2021 berate ich das Bundesamt für Justiz (BfJ) zur Lösung einer Problematik im Zusammenhang mit ausländischen Registerauskünften. Sensible Informationen werden in Einzelfällen an falsche Personen verschickt.**

In bestimmten Fällen ergänzt das BfJ als deutsche Registerbehörde Auskünfte aus dem Bundeszentralregister (BZR) mit einem Beitrag einer ausländischen Behörde, vor allem wenn die antragstellende Person die Staatsbürgerschaft eines anderen EU-Mitgliedsstaats besitzt. Diese Beiträge werden über das dezentral organisierte Europäische Strafregister-Informationssystem (ECRIS) eingeholt.

Bei der Erstellung Europäischer Führungszeugnisse gemäß § 30b Bundeszentralregistergesetz (BZRG) sind seit Juni 2021 Fälle aufgefallen, bei denen sich die Auskunft des anderen Mitgliedsstaats jeweils auf eine von der antragstellenden Person abweichende Person bezog. Dies betrifft verschiedene Staaten. Die Personen- und Registerdaten dieser anderen Personen haben ausländische Registerbehörden an das BfJ und dieses sodann an die antragstellenden Personen übermittelt. Es handelt sich entweder um genaue Informationen über im Ausland erfolgte Verurteilungen oder um die Information „keine Eintragung“. Im Ergebnis hat das BfJ sensible Daten anderer Personen an die antragstellenden Personen verschickt.

Auf Seiten des BfJ erfolgt bislang keine Prüfung der eingemeldeten ausländischen Auskunft, sie wird vollautomatisiert verarbeitet. Ein Abgleich der aus dem Ausland übermittelten Personendaten mit den Daten der antragstellenden Person findet nicht statt. Anteilig handelt es sich angesichts des umfangreichen Auskunftsbetriebs im BZR zwar nur um einen geringen Prozentsatz, die absolute Zahl von durchschnittlich etwa 15 Fällen jährlich ist aufgrund des individuellen Eingriffsgewichts erheblich und begründet Änderungsbedarf.

Entsprechend meiner Beratung ließ das BfJ mit erheblichem Aufwand einen Mechanismus programmieren, der



46 Urteil des Bundesverfassungsgerichts vom 1. Oktober 2024, Az. 1 BvR 1160/19, Rn. 158, 180; siehe auch 33. TB Nr. 7.4.4
47 https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2021/Positionspapier_Zweckbindung-Polizei.pdf?__blob=publicationFile&v=4
48 Urteil des Bundesverfassungsgerichts vom 1. Oktober 2024, Az. 1 BvR 1160/19, Rn. 158, 180
49 https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2025/19-Veranstaltung-P20.html

die ins Ausland übermittelten Personendaten mit den in der ausländischen Auskunft enthaltenen Personendaten abgleichen sollte. Wie im BZR üblich, sollten Zweifelsfälle von Sachbearbeitenden manuell geprüft werden. Dieser Mechanismus wurde aufgrund eines laut BfJ unverhältnismäßigen Personalaufwands nicht aktiviert. Das BfJ sieht sich nach erneuter Prüfung nicht mehr als datenschutzrechtlich (mit-)verantwortlich für die von ihm versandten ausländischen Auskünfte an.

Aus meiner Sicht wäre eine Lösung auf Ebene der ECRIS-RI zweckmäßig, dem EU-Rechtsrahmen für den Austausch von Registerinformationen zwischen EU-Staaten. Hierdurch könnte effektiv verhindert werden, dass eine ausländische Behörde überhaupt eine unzutreffende Auskunft versendet.

Sowohl seitens BfJ als auch meines Hauses wurde dieser Vorschlag in verschiedenen EU-Gremien bereits thematisiert. Dort besteht zwar Interesse daran, ob und wann es aber tatsächlich zu einer Änderung der ECRIS-RI kommen könnte, ist ungewiss. Bis zu einer Lösung auf EU-Ebene besteht Handlungsbedarf auf nationaler Ebene, erforderlichenfalls durch Bereitstellung angemessener Personalkapazitäten an das BfJ.

## 6.9 Visa-Informationssystem

**Das Auswärtige Amt (AA) und das Bundesverwaltungsamt (BVA) haben im Berichtsjahr aufgrund meiner Beratung eine Vereinbarung zur gemeinsamen datenschutzrechtlichen Verantwortlichkeit geschlossen.**

Im Juli 2025 haben das Auswärtige Amt (AA) und das Bundesverwaltungsamt (BVA) eine Vereinbarung über die gemeinsame datenschutzrechtliche Verantwortlichkeit für das Visa-Informationssystem (VIS)[50] abgeschlossen. Sie ist das Ergebnis eines konstruktiven Klärungs- und Beratungsprozesses, den meine Mitarbeiterinnen und Mitarbeitern nach einem Beratungs- und Kontrollbesuch im Jahr 2022 angestoßen haben.[51]

Ziel der Vereinbarung ist die rechtssichere Verarbeitung personenbezogener Daten im VIS. Einschließlich biometrischer Informationen ermöglicht das VIS den Austausch von Visadaten zwischen den Schengen-Staaten und dient in spezifischen Fällen auch Sicherheitsbehörden als Informationsquelle. Mit den vereinbarten Regelungen erfolgt eine rechtssichere Abgrenzung der jeweiligen Verpflichtungen der beteiligten Behörden. Das betrifft insbesondere die beim BVA liegende Zuständigkeit für die Bearbeitung von Auskunftsanträgen von Betroffenen.

Dank der intensiven Unterstützung durch meine Mitarbeiterinnen und Mitarbeiter werden die datenschutzrechtlichen Vorgaben durch die verantwortlichen Behörden nun umfassend gewährleistet. Dies erhöht die Rechtssicherheit aller Beteiligten und stärkt Deutschlands Position im Rahmen der anstehenden Evaluierung des Schengen-Besitzstands.

**Infokasten gemeinsame Verantwortlichkeit:**

Eine gemeinsame Verantwortlichkeit (auch „Joint Controllership“) liegt gemäß Art. 26 DSGVO vor, wenn zwei oder mehr Akteure zusammen über die Zwecke (das „Warum“) und die Mittel (das „Wie“) einer Datenverarbeitung entscheiden.



50 Informationen zum VIS unter: https://www.bfdi.bund.de/DE/Buerger/Inhalte/Inneres-Archive/Weiteres/EU-VIS.html
51 Vgl. 32. TB Nr. 9.2.4

# 7 Kontrollen und Maßnahmen



## Key Figures – Kontrollen und Maßnahmen

Vor-Ort-Kontrollen: 80
(– 4,8 % zum Vorjahr)

Schriftliche Kontrollen: 40
(+ 42,9 % zum Vorjahr)

Sonstige Kontrollen: 9
(+ 80 % zum Vorjahr)

Aufsichtsrechtliche Maßnahmen: 129
(+ 8,4 % zum Vorjahr)

Geldbußen: 45 177 500 Euro[52]

## 7.1 45 Millionen Euro Geldbußen gegen einen Telekommunikationsdiensteanbieter

**Ich habe einem Telekommunikationsdiensteanbieter aufgrund unzureichender Überprüfungen von Partneragenturen und Sicherheitsmängeln zwei Geldbußen in Höhe von 15 und 30 Millionen Euro auferlegt.**

Im Berichtsjahr habe ich gegen einen Telekommunikationsdiensteanbieter zwei Geldbußen in einer Gesamthöhe von 45 Millionen Euro erlassen.

Eine Geldbuße in Höhe von 15 Millionen Euro erging, weil das Unternehmen für sich tätige Partneragenturen nur unzureichend datenschutzrechtlich überprüft und überwacht hatte. Durch böswillig handelnde Mitarbeiterinnen und Mitarbeiter in Partneragenturen war es zu Betrugsfällen durch fingierte Verträge oder Vertragsänderungen zulasten von zahlreichen Kundinnen und Kunden gekommen.

Im Rahmen meiner Ermittlungen sah ich hier einen Verstoß gegen Art. 28 Abs. 1 S. 1 DSGVO. Danach dürfen Verantwortliche nur mit Auftragsverarbeitern zusammenarbeiten, welche hinreichende Garantien für den Datenschutz bieten. Im vorliegenden Fall waren die Partneragenturen nicht im ausreichenden Umfang datenschutzrechtlich überprüft und überwacht worden. Darüber hinaus waren Betrugsfälle durch Schwachstellen in bestimmten Vertriebssystemen begünstigt worden, wofür der Telekommunikationsdiensteanbieter verwarnt wurde.

Die zweite Geldbuße in Höhe von 30 Millionen Euro erging aufgrund von Schwachstellen im Rahmen eines Authentifizierungsprozesses bei der kombinierten Nutzung eines Onlineportals und der Hotline. Dadurch bestand das Risiko, dass unbefugte Dritte das eSIM-Profil und damit die Mobilfunknummer einer fremden Person übernehmen konnten. Dies hätte zur Folge gehabt, dass die eigentlich berechtigte Person von ihrem Profil und ihrer Rufnummer ausgeschlossen würde und sich eine unbefugte Person Zugriff auf weitere ihrer Online-Konten verschaffen kann. Denn viele Online-Dienste nutzen für eine Zwei-Faktor-Authentifizierung die Mobilfunknummer. Indem der Telekommunikationsdiensteanbieter den Zugang zu dem Kundenprofil nicht ausreichend gesichert hat, hat er gegen die Anforderungen der Datensicherheit nach Art. 32 Abs. 1 DSGVO verstoßen.

Den Geldbußen waren jahrelange aufsichtsbehördliche Ermittlungen vorausgegangen. Dabei haben meine Kontrolleurinnen und Kontrolleure u. a. Vor-Ort-Überprüfungen durchgeführt, Anwendungen und Systeme eingesehen sowie Dokumente ausgewertet. Das Unternehmen hat während der Dauer des gesamten Ver-

52 Gesamtvolumen der festgesetzten Geldbußen im Berichtsjahr.

fahrens ununterbrochen und uneingeschränkt mit mir kooperiert und auch Umstände offengelegt, durch die sich das Unternehmen selbst belastet hat. Es hat seine Prozesse und Systeme inzwischen deutlich verbessert und teilweise sogar vollständig ersetzt.

Die Kooperation im Rahmen der Ermittlungen und das Nachtatverhalten des Unternehmens bewerte ich als äußerst positiv und habe dies entsprechend bußgeldmindernd berücksichtigt. Das Unternehmen hat die Geldbußen akzeptiert und umgehend bezahlt. Ich werde die praktische Wirksamkeit der vom Telekommunikationsdiensteanbieter ergriffenen Maßnahmen in einer Folgekontrolle im Laufe des Jahres 2026 noch einmal überprüfen.

**Zur Übersicht der kontrollierten Stellen**

(QR-Code klicken oder scannen)

**Zur Übersicht der Maßnahmen**

(QR-Code klicken oder scannen)

## 7.2 Geldbußen in 177 500 Euro Gesamthöhe gegen einen Telekommunikationsdienste-anbieter

**Da ein Telekommunikationsdiensteanbieter in einer Vielzahl von Fällen Anfragen von Bürgerinnen und Bürgern zu ihren Betroffenenrechten meines Erachtens gar nicht oder nur unvollständig beantwortet hat, habe ich gegen ihn ein Bußgeld in einer Gesamthöhe von 177 500 Euro verhängt.**

Eine Vielzahl an Bürgerinnen und Bürgern wandte sich mit Beschwerden gegen einen Telekommunikationsdiensteanbieter an mich, der aus ihrer Sicht die ordnungsgemäße Erfüllung datenschutzrechtlicher Betroffenenrechte verweigerte.[53] Das Unternehmen versendete Briefe über vermeintlich abgeschlossene Verträge und in der Folge auch Mahnschreiben, obwohl Betroffene sich häufig überhaupt nicht daran erinnern konnten, einen Vertrag mit dem Anbieter geschlossen zu haben.

Soweit vermeintlich ein Vertrag über Telekommunikationsdienste zustande gekommen ist, liegt die Zuständigkeit bei mir. Für davor liegende Sachverhalte liegt die Zuständigkeit bei der Landesdatenschutzaufsicht.

Sofern die Betroffenen gegenüber dem Unternehmen ihre Rechte nach der DSGVO geltend machten, erhielten sie oftmals gar keine oder nach meiner Einschätzung nur eine unvollständige Antwort. Insbesondere machte der Anbieter bei Auskunftsverlangen der Bürgerinnen und Bürger keine Aussagen dazu, woher er die personenbezogenen Daten der Betroffenen für die ersten Anschreiben hatte. Hierzu ist er jedoch verpflichtet. Im Rahmen der Auskunft muss Betroffenen neben den in Art. 15 Abs. 1 DSGVO genannten Angaben zudem eine Kopie ihrer personenbezogenen Daten in Sinne einer originalgetreuen Reproduktion bereitgestellt werden, soweit dies für die Ausübung der Betroffenenrechte erforderlich ist. Das Auskunftsrecht dient dazu, Betroffenen einen Überblick und die Kontrolle über die Verarbeitung ihrer personenbezogenen Daten zu ermöglichen, damit sie auch selbst prüfen können, ob ihre Daten rechtmäßig verarbeitet werden.

Aufgrund der Beschwerden habe ich gegen das Unternehmen Untersuchungen eingeleitet, soweit es meine Zuständigkeit betrifft. In vielen Fällen habe ich den Anbieter in der Folge angewiesen, die Rechte der Betroffenen ordnungsgemäß zu erfüllen. Einige dieser Anweisungen sind bereits bestandskräftig geworden, müssen jedoch teilweise mithilfe von Zwangsgeldern durchgesetzt werden. In anderen Fällen hat das Unternehmen Klage gegen meine Aufsichtsmaßnahmen eingelegt, so dass diese Fälle derzeit vor Gericht verhandelt werden.

Für zunächst 22 der ermittelten Verstöße habe ich abhängig von deren Schwere zudem jeweils Geldbußen zwischen 7 500 und 20 000 Euro erlassen. Gegen diesen Bußgeldbescheid mit einer Gesamthöhe von 177 500 Euro hat das Unternehmen Einspruch eingelegt, den ich als unbegründet bewertet habe. Der Fall wurde daher zur Durchführung eines gerichtlichen Bußgeldverfah-

53 33. TB Nr. 8.2.3

rens an die zuständige Staatsanwaltschaft weitergeleitet. Eine gerichtliche Klärung des Falles steht noch aus.

## 7.3 Einigung im ePA-Verfahren

**Bereits 2021 hat mein Vorgänger gegen mehrere Krankenkassen Anweisungen in Bezug auf die Ausgestaltung des Zugriffsmanagements der ePA erlassen.[54] Mit den betroffenen Krankenkassen konnten in den gegen diese Bescheide erhobenen Klageverfahren nun Einigungen erzielt werden.**

Mit Anweisungen an Krankenkassen sollte sichergestellt werden, dass den Patientinnen und Patienten die größtmögliche Souveränität über die Verwendung der sie betreffenden personenbezogenen Daten im Rahmen der elektronischen Patientenakte (ePA) gewährt und die Datenschutzgrundsätze der DSGVO befolgt werden. Den Kassen wurde daher aufgegeben, das Zugriffsmanagement der ePA feingranular auszugestalten und auch Patientinnen und Patienten ohne eigene technische Endgeräte den Zugriff auf die ePA zu ermöglichen, die sie betreffenden personenbezogene Daten einsehen zu können, ohne dass sie dafür eine dritte Person als ihren Vertreter bestellen müssen. Gegen diese Anweisungen hatten Krankenkassen Klagen erhoben.

In diesen Verfahren konnte ich Einigungen erzielen. Entscheidend dafür waren zwischenzeitlich erfolgte Änderungen der für die ePA relevanten Rechtsgrundlagen. Die Verarbeitung der personenbezogenen Daten bedarf danach keiner expliziten Einwilligung der Versicherten mehr, sondern beruht nun auf einem gesonderten gesetzlichen Erlaubnistatbestand, der den Patientinnen und Patienten ein Widerspruchsrecht einräumt.

Nach der erzielten Einigung werden die betroffenen Krankenkassen darauf hinwirken, die Möglichkeiten zur Einsichtnahme in die ePA durch Versicherte, denen kein Zugriff über eigene Endgeräte möglich ist, weiter zu stärken.

**Querverweis:**

3.1.2 Bundesweiter Rollout der ePA

## 7.4 VG Köln zur Facebook-Fanpage der Bundesregierung

**Im Juli 2025 erging von dem Verwaltungsgericht (VG) Köln das erstinstanzliche Urteil zur Untersagungsverfügung aus dem Jahr 2023, mit der der Betrieb der Facebook-Fanpage der Bundesregierung durch das Bundespresseamt (BPA) wegen Verstößen gegen das Datenschutzrecht verboten wurde.**

In einem Bescheid aus dem Jahr 2023 hatte mein Vorgänger dem BPA den Betrieb der Facebook-Fanpage für die Bundesregierung untersagt.[55] Die Maßnahme basierte auf einem Kurzgutachten der Datenschutzkonferenz (DSK), das zu dem Ergebnis kam, dass die Betreiber von Facebook-Fanpages und Meta gemeinsam für die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Betrieb der Facebookseite der Bundesregierung verantwortlich seien. Die Einschätzung des DSK-Kurzgutachtens geht u. a. auf die Wirtschaftsakademie-Entscheidung des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018 (Az. C-210/16) und deren Weiterentwicklung in einer Vielzahl von anderen Urteilen[56] zurück. Vor diesem Hintergrund wären dem BPA Verstöße gegen das Datenschutzrecht zuzurechnen, die mit der Verarbeitung im Kontext der Fanpage der Bundesregierung im Zusammenhang stehen. Solche Verstöße lagen in Form der Nichterfüllung von Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO sowie aufgrund fehlender Einwilligungen in Datenverarbeitungen nach Art. 6 Abs. 1 Buchst. a DSGVO und § 25 TDDDG vor. Gegen den erlassenen Bescheid erhoben sowohl das BPA als auch die Meta Platforms Ireland Ltd. (Meta), die nicht Adressatin des Bescheids war, Klage vor dem VG Köln.

Das Gericht hat den Bescheid gegen das BPA in seinem Urteil vom 17. Juli 2025 (Az. 13 K 1419/23) aufgehoben. Die Klage von Meta wurde hingegen in drei von vier Punkten abgewiesen. Zur Begründung führt das Gericht aus, dass das BPA nicht mit Meta gemeinsam datenschutzrechtlich für die Verarbeitung der personenbezogenen Daten nach der DSGVO verantwortlich sei, da die Mittel der Datenverarbeitung nicht von beiden gemeinsam festgelegt würden. Ferner sei das BPA nicht für das Einholen einer Einwilligung der Nutzerinnen und Nutzer zum Platzieren von Cookies verantwortlich, weil durch den Betrieb der Facebookseite kein ausreichender Ursachen- und Wirkungszusammenhang zur Cookieset-



54 30. TB Nr. 6.1
55 Vgl. 32. TB Nr. 8.5
56 Urteil vom 10.07.2018, Az. C-25/17, Urteil vom 29.07.2019, Az. C-40/17, Urteil vom 05.12.2023, Az. C-683/21, oder auch Urteil vom 11.01.2024, Az. C-231/22)

zung hergestellt werde. Nach Ansicht des Gerichts könne das BPA daher nicht Adressat einer datenschutzrechtlich begründeten Untersagungsverfügung sein. Es ließ die Berufung gegen sein Urteil zu. Nach ausführlicher Prüfung der gerichtlichen Entscheidung habe ich mich entschlossen, Berufung gegen das Urteil beim Oberverwaltungsgericht (OVG) Nordrhein-Westfalen einzulegen.

Ich möchte betonen, dass es mir zu keiner Zeit darum ging, öffentlichen Stellen die Kommunikation über soziale Medien zu verbieten. Ganz im Gegenteil. Aber Bürgerinnen und Bürger müssen sich darauf verlassen können, dass staatlich genutzte Plattformen nicht rechtswidrig mit ihren Daten verfahren. Dies gewährleisten kann nur eine höchstrichterliche Entscheidung in der konkreten Frage. Ein paralleles Verfahren mit vergleichbaren Fragen ist derzeit vor dem VG Dresden rechtshängig.

Zugleich ist es mir wichtig, dass die bei vielen öffentlichen Stellen bestehende Verunsicherung in Bezug auf die rechtmäßige Nutzung sozialer Medien beseitigt wird. Selbstverständlich respektiere ich die durch das Urteil des VG Köln geschaffene Rechtslage, die es öffentlichen Stellen bis zu einer endgültigen Klärung durch den Gesetzgeber oder die Gerichtsbarkeit ermöglicht, Social Media ohne Bedenken vor eventuell drohenden Maßnahmen der Datenschutzaufsicht zu nutzen. Deshalb habe ich mit meiner Handreichung zur Nutzung sozialer Netzwerke durch öffentliche Stellen des Bundes konkrete Handlungshinweise gegeben.

**Handreichung zur Nutzung sozialer Netzwerke durch öffentliche Stellen des Bundes**

(QR-Code klicken oder scannen)

## 7.5 VG Köln bestätigt Rechtmäßigkeit der Abhilfemaßnahmen gegen das THW

**Während der COVID-19-Pandemie hatte das Technische Hilfswerk (THW) begonnen, den Impfstatus sämtlicher Beschäftigten zu erheben, unabhängig davon, ob sie Verwaltungsaufgaben im Innendienst erledigten oder im Außendienst tätig waren. Die daraufhin von mir gegen das THW ergriffenen Aufsichtsmaßnahmen sind durch das VG Köln mit Urteil vom 31. Juli 2025 bestätigt worden.**

Um ihre Funktionsfähigkeit aufrecht zu erhalten, dürfen Einrichtungen von besonderer Bedeutung nach Art. 9 Abs. 2 Buchst. i DSGVO i. V. m. § 23a S. 1 Infektionsschutzgesetz (IfSG) den Impf- und Serostatus eines Beschäftigten verarbeiten. Das THW gehört allerdings nicht zu den privilegierten Einrichtungen. Aus diesem Grunde hatte ich mehrere Abhilfemaßnahmen gegen das THW erlassen: die Untersagung der Datenerhebung, die Löschung bereits erhobener Daten und eine Verwarnung für die vorwerfbare Missachtung des Gesetzes.

Das THW hatte Anfechtungsklage gegen diese Maßnahmen erhoben. Dies führte rechtlich dazu, dass die Anordnungen bis zu einer Gerichtsentscheidung ausgesetzt waren. Zwar kann ich gegen Unternehmen in bestimmten dringlichen Fällen die sog. sofortige Vollziehung anordnen, so dass Anordnungen dann auch im Falle eines laufenden Gerichtsverfahrens zu befolgen sind. Eine entsprechende Anordnung der sofortigen Vollziehung gegenüber Behörden hat der Gesetzgeber in § 20 Abs. 7 BDSG jedoch ausgeschlossen. Während der COVID-19-Pandemie konnte das THW die personenbezogenen Daten daher weiter erheben und verarbeiten – rechtswidrig, wie das VG Köln mit Urteil vom 31. Juli 2025 (13 K 3809/21) bestätigte.

Dieser Fall zeigt, dass die Privilegierung von Behörden in § 20 Abs. 7 BDSG die Effektivität der DSGVO beeinträchtigt. Hierdurch wird es ermöglicht, dass Behörden – anders als Unternehmen – aus meiner Sicht rechtswidrige Verarbeitungen weiter vornehmen können, ohne dass ich dies verhindern kann. Nach meiner Einschätzung ist dies mit dem Effektivitätsgebot des Unionsrechts und dem Grundrechtsschutz der betroffenen Personen nicht vereinbar.

**Ich wiederhole daher meine Empfehlung gegenüber dem Gesetzgeber, die unionsrechtswidrige Vorschrift des § 20 Abs. 7 BDSG zu streichen.**

## 7.6 Datenschutzkontrolle beim Bundesnachrichtendienst

**Vor der anstehenden Gesetzesreform bei den Nachrichtendiensten, in der auch deren Kontrolle restrukturiert werden soll, belegt die Aufsichtstätigkeit der BfDI beim Bundesnachrichtendienst (BND) in 2025 den Wert einer über Jahre eingespielten und auf erarbeitetem Fachwissen basierenden Kontrolle. Eine Reform muss darauf achten, das derzeitige Datenschutzniveau zu halten.**

**In sechs Bereichen habe ich beim BND im Berichtsjahr Datenschutzverstöße festgestellt. Zudem setzt sich die Auskunftsverweigerungshaltung des BND fort: In zwei Fällen konnte die Einhaltung von Datenschutzvorschriften nicht überprüft werden, da mir Unterlagen vorenthalten worden sind. In einer Kontrolle haben mir unvollständige Protokolldaten die Prüfung erschwert.**

Im 33. Tätigkeitsbericht habe ich mich zu Plänen der Bundesregierung geäußert, in einer grundlegenden Reform des Nachrichtendiensterechts auch die Landschaft der Kontrollorgane zu restrukturieren.[57] Ich sorge mich, dass wegen der gegenwärtigen Sicherheitsbedrohungen für Deutschland die Interessen der nationalen Sicherheit zu einseitig in den Fokus genommen werden und dadurch die rechtsstaatliche Kontrolle der Nachrichtendienste nachhaltig geschwächt wird.

**Festgestellte Datenschutzverstöße**

Die Beratungs- und Kontrolltätigkeit meines Hauses beim BND im Jahr 2025 zeigt deutlich, dass es eine eigenständige, unabhängige und erfahrene Aufsicht über die Nachrichtendienste geben muss, die gerade die Einhaltung des Datenschutzrechts überwacht. In sechs verschiedenen Bereichen sind Verstöße im Datenschutz festgestellt worden:

In einem Bereich verarbeitet der BND massenhaft Daten, ohne dass es dafür eine belastbare Gesetzesgrundlage gibt, die gemessen am Parlamentsvorbehalt frei von Zweifeln ist. Bei diesen Verarbeitungen sind auch in einem großen Umfang Daten von deutschen Staatsangehörigen betroffen.

Des Weiteren hat eine meiner Kontrollen einer Datei des BND u. a. ergeben, dass in erheblichem Umfang die gesetzlich vorgeschriebenen Löschwiedervorlagefristen nicht eingehalten worden sind. Der BND hat in dieser Datei nicht flächendeckend in den gesetzlich vorgesehenen Abständen die Überprüfung gewährleistet, ob die erfassten Personen und die zu ihnen gespeicherten personenbezogenen Daten noch für die Arbeit des BND erforderlich sind.

In Bezug auf eine andere Datei hat der BND nach Ankündigung eines Informationsbesuches zu dieser Datei gemeldet, dass bedingt durch das Fehlen einer funktionierenden Löschroutine seit Mitte 2023 keine Daten mehr gelöscht und in der Folge in beträchtlichem Ausmaß personenbezogene Daten unrechtmäßig zu lange gespeichert worden sind. Der BND hat der BfDI im Informationstermin ein Vorgehen vorgestellt, wie in der betreffenden Datei u. a. durch vor Ort vorgenommene Löschungen ein datenschutz- und damit grundrechtskonformer Zustand wieder hergestellt werden kann.

Kontrolliert worden ist auch der Bereich der Bearbeitung von Auskunftsersuchen nach § 9 BNDG, § 15 BVerfSchG und Art. 15 DSGVO. Festgestellt habe ich hier insbesondere, dass der BND nicht alle seine durchsuchbaren automatisierten Dateien, in denen personenbezogene Daten verarbeitet werden, tatsächlich durchsucht und in der Folge eine Beauskunftung im gesetzlich vorgeschriebenen Umfang nicht immer gewährleistet hat. Der BND hat meinen Kontrollfeststellungen zum Beauskunftungsumfang widersprochen und ist der Auffassung, es seien technische und organisatorische Maßnahmen zur Sicherstellung des Auskunftsanspruches seitens der BfDI nicht berücksichtigt worden. Der Widerspruch geht am festgestellten Datenschutzverstoß vorbei, weil die unstreitige Nichtdurchsuchung von einigen automatisierten Dateien des BND nicht durch technische und organisatorische Maßnahmen kompensiert werden kann.

Gegenstand einer weiteren Kontrolle waren Übermittlungen zur politischen Unterrichtung gemäß § 65 Abs. 1 BNDG. In einer Vielzahl von Fällen hat der BND Übermittlungen fälschlicherweise auf § 65 Abs. 1 BNDG gestützt.

Eine Kontrolle des behördlichen Datenschutzes hat schließlich u. a. ergeben, dass die Weisungsfreiheit des behördlichen Datenschutzes gemäß Art. 38 Abs. 3 DSGVO aufgrund der Verortung in der Linienorganisation und einer fehlenden hinreichenden Trennung zu anderen Sachgebieten nicht gegeben gewesen ist und dass die tatsächliche personelle Ausstattung nicht den Anforderungen an die erforderlichen Ressourcen gemäß Art. 38 Abs. 3 DSGVO genügte. Der BND hat in Ansehung der Kontrollfeststellungen die Organisation und Ausgestaltung des behördlichen Datenschutzes entsprechend meiner Hinweise so verändert, dass er den gegenständlichen Vorgaben von Art. 38 DSGVO nunmehr entspricht.

**Auskunftsverweigerung**

Auch in 2025 konnte ich meiner gesetzlichen Kontrollaufgabe, die von Verfassungs wegen geboten ist, nicht vollumfänglich nachkommen, weil mir BND und das Bundeskanzleramt als BND-Fachaufsicht teilweise die Einsichtnahme in Unterlagen verweigern und notwendige Informationen vorenthalten. Die zu kontrollierende Stelle maßt sich auf diese Weise an zu entscheiden, was kontrolliert wird und was nicht. Wegen dieser Kon-

57 Vgl. 33. TB Nr. 3.3.2

trollvereitelung konnte ich in 2025 u. a. beispielsweise nicht die Einhaltung der Vorschriften zur Auftragsverarbeitung (§ 62 BDSG) und zu den Anforderungen an die Sicherheit der Datenverarbeitung (§ 64 BDSG), die für den BND gemäß § 64 Nr. 2 BNDG gelten, in Bezug auf bestimmte Gegebenheiten prüfen. BND und Bundeskanzleramt erwarten insoweit, dass ihre Aussagen und datenschutzrechtlichen Bewertungen von der BfDI als gesetzlich vorgesehene unabhängige Kontrollbehörde ungeprüft hingenommen werden. Im Rahmen der Durchführung der Kontrolle zur politischen Unterrichtung habe ich außerdem durch vorgenommene Löschungen des behördlichen Datenschutzes des BND unvollständige Protokolldaten erhalten, was die Auswahl der im Anschluss an die Protokolldatenauswertung inhaltlich geprüften Übermittlungen erschwert hat.

**Querverweise:**

3.3.1 Gesetzgebungsvorhaben – Polizei, Nachrichtendienste und Sicherheits- sowie Zuverlässigkeits- und Verfassungstreueprüfungen, 7.7 Betroffenenrechte bei Polizeibehörden und Nachrichtendiensten

## 7.7 Betroffenenrechte bei Polizeibehörden und Nachrichtendiensten

**Wie steht es um die Gewährleistung der Betroffenenrechte bei den Polizeibehörden und Nachrichtendiensten des Bundes? Die Abteilung SI hat dieses Thema im Jahr 2025 zu einem ihrer Schwerpunkte erklärt und verstärkt Beratungen und Kontrollen hierzu durchgeführt.**

Die Rechte der betroffenen Personen auf Auskunft über ihre gespeicherten Daten und gegebenenfalls Löschung sind zentrale Rechte des Datenschutzes. Die Gewährleistung der Betroffenenrechte ist auch weiterhin eines meiner zentralen Anliegen, weshalb meine Mitarbeiterinnen und Mitarbeiter der Abteilung Sicherheit (SI) in diesem Jahr den Umgang mit den Betroffenenrechten im Rahmen von Beratungen, Kontrollen oder Informationsbesuchen bei dem Zollkriminalamt (ZKA), der Financial Intelligence Unit (FIU), der Zentralstelle für Sanktionsdurchsetzung (ZfS), der Bundespolizei (BPOL), dem Bundesnachrichtendienst (BND), dem Bundeskriminalamt (BKA), der Polizei des Deutschen Bundestages (BTPOL), dem Bundesamt für den militärischen Abschirmdienst (BAMAD) und dem Bundesamt für Verfassungsschutz (BfV) untersucht haben. Die Kontrolle beim BKA ist aktuell noch nicht abgeschlossen, daher kann ich dazu nur einige Punkte herausgreifen.

Die Betroffenenrechte werden jährlich von mehreren tausend Bürgerinnen und Bürgern aktiv ausgeübt – die Tendenz ist steigend. Im Jahr 2025 wurden allein beim BKA circa 9000 **Anträge auf Auskunft und Löschung** gestellt. Meine Mitarbeiterinnen und Mitarbeiter stellten im Wesentlichen eine umsichtige und gewissenhafte Bearbeitung der Anträge durch die Sicherheitsbehörden fest. Trotzdem gab es einige Mängel. So ist die pauschale Anforderung von Ausweiskopien oder deren Speicherung in den Vorgängen bei vielen Sicherheitsbehörden ein Kritikpunkt (ZKA, BPOL, BND, BKA, BAMAD).

Bei den Behörden, deren gesetzliche Grundlagen der Richtlinie EU 2016/680 (JI-Richtlinie) unterliegen (ZKA, BPOL, BKA) und die daher im Bereich der Betroffenenrechte die §§ 55 ff. Bundesdatenschutzgesetz (BDSG) zu beachten haben, dient die Ausweiskopie der Identitätsfeststellung der Antragstellenden. Sie darf nur bei begründeten Zweifeln an der Identität angefordert werden und nur zu diesem Zweck, also bis zur erfolgten Identitätsfeststellung, vorgehalten werden.

Bei den Untersuchungen stellte meine Behörde jedoch fest, dass die Ausweiskopien häufig angefordert wurden, obwohl kein begründeter Zweifel an der Person des Antragstellers vorlag (ZKA, FIU, BPOL). Häufig wurde die Ausweiskopie zudem für die gesamte Speicherdauer des Bearbeitungsvorgangs vorgehalten (BPOL, BAMAD, BND, BKA). Das sind je nach Behörde zwischen drei und fünf Jahren. Im Zuge meiner Beratung konnte ich erreichen, dass die BPOL ihr Verfahren umstellte und nun die Ausweiskopien nach erfolgter Identitätsfeststellung aus den Bearbeitungsvorgängen zu den Betroffenenrechten entfernt und dies im Vorgang kurz dokumentiert. Auch beim ZKA konnte ich sensibilisieren. Hier werden künftig qualifizierte elektronische Signaturen anerkannt und die Ausweiskopien nach erfolgter Identitätsfeststellung gelöscht. Das BKA hingegen speichert die Ausweiskopien derzeit noch für 36 Monate nach Abschluss des Bearbeitungsvorgangs, das BAMAD speichert die Ausweiskopien in den Vorgängen bis zum Vorgangsende (regelmäßig fünf Jahre). Hierzu stehe ich mit beiden Behörden im Austausch, um eine Veränderung der Praxis zu erreichen.

Der bei einer Auskunftsverweigerung nach § 57 Abs. 7 BDSG erforderliche Hinweis auf das **Recht, die BfDI anzurufen**, fehlte bei den vom ZKA und der BTPOL erstellten Bescheiden, ebenso wie die Information, **gerichtlichen Rechtsschutz** ersuchen zu können. Bei der BPOL und dem BKA fehlten diese Hinweise in den Fällen von Auskunftsverweigerungen teilweise. Beide Informationen sind für betroffene Personen jedoch zur Wahrung ihrer Rechte wichtig.

Bei der BPOL und der FIU wurden die Anträge auf Auskunft und die Anträge auf Löschung nicht immer klar differenziert. So wurde vereinzelt ein Löschantrag nicht als solcher verstanden und nur als Auskunftsantrag bearbeitet.

Der BND durchsucht bei **Auskunftsersuchen** nach § 9 BNDG i. V. m. § 15 BVerfSchG nicht sämtliche bei ihm betriebenen automatisierten Dateien, in denen personenbezogene Daten von Auskunftsersuchenden enthalten sein könnten. Unabhängig von den bestehenden gesetzlichen Auskunftsverweigerungsgründen des § 15 BVerfSchG kann nicht pauschal argumentiert werden, dass die vollständige Suche einen unverhältnismäßigen Aufwand darstellt. Die Frage eines etwaigen unverhältnismäßigen Verwaltungsaufwandes für die Beantwortung eines Auskunftsantrages kann letztlich erst nach Kenntnis des konkreten Trefferumfangs beantwortet werden.

Bei einzelnen Stellen traten weitere Mängel auf: Es gab Dokumentationsdefizite beim BfV, der BPOL und der FIU. Beim ZKA und der FIU wurden Vorgänge doppelt geführt, was mit der Einführung der elektronischen Akte behoben wird.

Einige der festgestellten Mängel haben die geprüften Stellen direkt behoben, zu den weiteren Mängeln stehe ich mit den Behörden noch im Austausch. Insgesamt hat der Prüfungsschwerpunkt der Abteilung SI das Bewusstsein für die Rechte der Betroffenen bei den beaufsichtigten Behörden geschärft. Als Hilfestellung für die Behörden wird derzeit von meinem Haus eine behördenübergreifende Handreichung für die Bearbeitung von Auskunfts- und Löschanträgen erarbeitet.

Parallel war mein Haus auch auf EU-Ebene im Sinne der Betroffenen aktiv. Meine Mitarbeiterinnen und Mitarbeiter arbeiteten im Europäischen Datenschutzausschuss (EDSA) federführend an Leitlinien zum Auskunftsrecht nach der JI-Richtlinie mit. Die Leitlinien behandeln eine Vielzahl von zentralen und praxisrelevanten datenschutzrechtlichen Fragen und dienen damit der europaweiten Stärkung und Harmonisierung der Betroffenenrechte.

**Querverweis:**

7.6 Datenschutzkontrolle beim Bundesnachrichtendienst

## 7.8 Kontrollen beim BKA

**Ich habe im Berichtsjahr datenschutzrechtliche Kontrollen beim Bundeskriminalamt (BKA) durchgeführt und u. a. OSINT, die DNA-Analysedatei, Zugriffe auf Daten im Informationssystem und den Informationsverbund sowie das eFBS geprüft.**

Im Jahr 2025 habe ich einen Beratungs- und Kontrollbesuch zu Ermittlungen mittels **Open Source Intelligence (OSINT) Recherchen** beim BKA durchgeführt. Die datenschutzrechtliche Prüfung von OSINT hat keine Datenschutzverstöße aufgezeigt. Jeder Person, und damit auch jeder Behörde, stehen zahlreiche Informationen aus Printmedien, dem Rundfunk, dem Internet oder aus webbasierten Anwendungen zur Verfügung. Ermittlungsbehörden können diese frei zugänglichen Informationen für ihre Recherchen nutzen.

Die Recherche aus frei zugänglichen Quellen kann in das Recht auf informationelle Selbstbestimmung eingreifen, insbesondere wenn eine Ermittlungsbehörde allgemein zugängliche Informationen gezielt zusammenträgt, speichert, auswertet und ggf. weitere Daten hinzuzieht. Daraus kann sich eine besondere Eingriffstiefe in das Persönlichkeitsrecht der betroffenen Person ergeben. Hierfür bedarf es einer Ermächtigungsgrundlage.

Eine spezialgesetzliche Ermächtigungsgrundlage für die sog. OSINT-Recherchen existiert im Bereich des strafrechtlichen Ermittlungsverfahrens nicht. Es sind deshalb die Generalklauseln der §§ 161, 163 Abs. 1 Strafprozessordnung (StPO) heranzuziehen. In den von mir eingesehenen Vorgängen konnte die Recherche auf diese Vorschriften gestützt werden. Sie waren noch nicht von einer solchen Eingriffsintensität, dass dafür eine spezialgesetzliche Rechtsgrundlage notwendig gewesen wäre. Ein solcher Eingriff in das Recht auf informationelle Selbstbestimmung, der nur durch eine spezialgesetzliche Rechtsgrundlage zu legitimieren ist, liegt etwa dann vor, wenn eine staatliche Stelle in zugangsgesicherte Kommunikationsinhalte mittels Zugriffsdaten vordringt, die sie gegen oder ohne Willen eines Berechtigten erlangt hat. Gleiches kann gelten, wenn Daten automatisiert abgeglichen werden. Insbesondere sind auch die Grenzen des § 110a StPO zu beachten, wenn Beamte im Internet unter einer Legende ermitteln.

Die **Kontrolle der DNA-Analysedatei** des BKA hat keine erheblichen datenschutzrechtlichen Mängel gezeigt.

In meiner Stichprobe habe ich mir auch Fälle angesehen, in denen das BKA Datensätze zu einer Person aus der DNA-Analysedatei von einer Landespolizeibehörde übernommen hat. Dies geschieht in der Regel, wenn die Landespolizei beabsichtigt, den von ihr gespeicherten Datensatz aus der DNA-Analysedatei zu löschen. Das BKA darf den Datensatz nur dann als eigenen übernehmen, wenn es bereits vor der Löschung über eigene ausreichende Erkenntnisse verfügt, die zum Zeitpunkt der

Übernahme des Datensatzes die gesetzlichen Voraussetzungen erfüllen.

In den von mir geprüften Fällen waren die gesetzlichen Anforderungen erfüllt, insbesondere die des § 81g Abs. 1 StPO. Gemäß dieser Vorschrift dürfen zur Identitätsfeststellung in künftigen Strafverfahren Körperzellen nur dann entnommen und molekulargenetisch untersucht werden, wenn wegen der Art oder Ausführung der Tat, der Persönlichkeit der oder des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen sie oder ihn künftig Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sind. In diesen Fällen muss das BKA sog. Negativprognosen dokumentieren.

In diesem Zusammenhang fiel mir positiv auf, dass das BKA bemüht ist, seine Arbeitsabläufe zu optimieren. Ich sehe allerdings noch Möglichkeiten, die Dokumentation insofern zu verbessern. Einheitliche Ablageorte können dafür sorgen, dass sich die Dokumentation leichter auffinden lässt. Bislang befanden sich die Negativprognoseentscheidungen an unterschiedlichen Speicherungsorten. Hierdurch war es dem BKA zunächst nicht möglich, meinen Mitarbeitenden alle erforderlichen Negativprognoseentscheidungen vorzulegen, dies gelang erst im Nachgang des Besuchs. In wenigen Fällen habe ich die Prognoseentscheidung nicht als ausreichend betrachtet und das BKA um Ergänzungen gebeten. Das BKA hat einige Fälle daraufhin gelöscht oder die Prognoseentscheidung ergänzt, weshalb ich von einer Beanstandung abgesehen habe.

Die **Kontrolle von Zugriffen** hat keine Mängel ergeben. Der polizeiliche Informationsverbund enthält sensible Informationen über Personen. Es ist daher sicherzustellen, dass Beamtinnen und Beamte nur zur Erfüllung der dienstlichen Pflichten auf diese Daten zugreifen können. Ich habe die gesetzliche Aufgabe, dies alle zwei Jahre zu überprüfen. Der gesetzliche Kontrollauftrag ist allerdings eher auf den künftigen polizeilichen Informationsverbund zugeschnitten, der mit dem Gesamtprogramm Polizei 20/20 (P 20) angestrebt wird. Mit dem in §§ 12 ff. BKAG vorgesehenen Konzept ist künftig eine höhere Prüftiefe möglich. Derzeit stehen das neue Informationssystem und der nach § 29 BKAG vorgesehene Informationsverbund noch nicht in der vom Gesetzgeber vorgesehenen Form zur Verfügung. Um meinem Kontrollauftrag gerecht zu werden, haben meine Mitarbeiterinnen und Mitarbeiter eine umfangreiche Stichprobe von Zugriffen auf das Informationssystem INPOL-Z eingesehen. Zudem haben sie die bereits vorhandenen Kontrollmechanismen und -konzepte des BKA vor Ort überprüft. Es konnten keine rechtswidrigen Zugriffe festgestellt werden.

In meiner Kontrolle des **einheitlichen Fallbearbeitungssystems des BKA (eFBS)** habe ich keine Datenschutzverstöße festgestellt, sehe aber Verbesserungspotenzial bei der Datenqualität, den Zugriffsberechtigungen und den Anforderungen an die Löschvorgaben.

**Querverweis:**

6.7 Polizei 20/20 (P20)

## 7.9 Beratung und Kontrolle des BfV und des MAD

**Auch in diesem Berichtsjahr waren Einführungen oder Anpassungen von automatisierten Dateien Gegenstand der Beratungs- und Kontrolltätigkeit beim Bundesamt für Verfassungsschutz (BfV). Beim Militärischen Abschirmdienst (MAD) hat mein Haus die Kontrolle des Nachrichtendienstlichen Informationssystems ohne Beanstandungen abgeschlossen und begleitet u. a. die Einführung neuer, teilweise auf Künstlicher Intelligenz (KI) basierender Systeme.**

**Dokumentation beim BfV**

In den vergangenen Jahren und erneut im Jahr 2025 hat mein Haus bei verschiedenen Prüfungen eine unzureichende Dokumentation des Verwaltungshandelns beim Bundesamt für Verfassungsschutz (BfV) festgestellt. Meine Mitarbeiterinnen und Mitarbeiter sind seither bemüht, das BfV und das Bundesministerium des Innern (BMI) davon zu überzeugen, dass eine Dokumentation des Verwaltungshandelns elementarer Bestandteil der behördlichen Tätigkeit ist. Dies gilt im besonderen Maße für die Arbeit der Nachrichtendienste, die auf zum Teil sehr weit formulierten rechtlichen Grundlagen beruhen, die in der Praxis der Auslegung bedürfen.

BMI und BfV vertreten die Auffassung, dass es ausreichend sei, die Durchführung der Ermessensentscheidung zu dokumentieren. Die maßgeblichen Erwägungen selbst müssten hingegen nicht nachprüfbar dokumentiert werden. Da es an einer einfachgesetzlichen Pflicht zur Dokumentation mangele, wird außerdem meine diesbezügliche Berechtigung zur Beanstandung insofern in Frage gestellt.

Im Ergebnis führen die Mängel in der Dokumentation dazu, dass eine Überprüfung der Rechtmäßigkeit des Verwaltungshandelns nicht oder nur mit erheblichen Einschränkungen möglich ist. Dies wirkt sich unmittelbar auf die datenschutzrechtlichen Prüfungen aus. Durch die Hinzuziehung der jeweils zuständigen Fachkräfte vergrößert sich der Aufwand, gleichzeitig müssen

meine Mitarbeiterinnen und Mitarbeiter ohne Dokumentationen den Ausführungen des BfV vertrauen. Erst recht gilt dies, wenn die mündliche Erläuterung nur mit viel gutem Willen aus dem schriftlichen Vorgang herauszulesen ist. Dies ist nicht zufriedenstellend.

Die Dokumentation dient nicht nur der Datenschutzkontrolle. Sie ermöglicht auch die parlamentarische Kontrolle, die Wahrnehmung der Rechtsaufsicht, die gerichtliche Überprüfung im Einzelfall und die Sicherstellung des behördeninternen Wissenstransfers.

**Im Rahmen der Novellierung des Nachrichtendienstrechts sollte die Dokumentationspflicht festgeschrieben werden, um eine unabhängige Kontrolle im erforderlichen Rahmen zu ermöglichen.**

**Dateisysteme beim BfV**

Sofern das BfV personenbezogene Daten in Dateien speichern möchte, ist mein Haus vor Inbetriebnahme der Datei im Rahmen eines Dateianhörungsverfahrens gemäß § 14 BVerfSchG zu beteiligen. In diesem Berichtsjahr waren meine Mitarbeiterinnen und Mitarbeiter mit einem Dateisystem befasst, das für die automatisierte Auswertung und Analyse großer Datenmengen im BfV eingeführt werden soll. Bei einem Informationstermin konnten meine Mitarbeiterinnen und Mitarbeiter feststellen, dass sich das BfV um die Gestaltung eines datenschutzkonformen Systems bemüht.

Im Ergebnis wird der Bedarf am Einsatz von modernen technischen Analysemethoden von meinem Haus nicht in Frage gestellt. Das BfV sieht sich, wie alle Sicherheitsbehörden, mit der stetigen Weiterentwicklung der Social-Media-Plattformen sowie mit der häufig wechselnden Art der Nutzung der verschiedenen Kommunikationswege konfrontiert. Es ist für das BfV unmöglich, die dabei entstehenden großen Datenmengen ausschließlich durch Mitarbeiterinnen und Mitarbeiter ohne technische Unterstützung auszuwerten und zu analysieren. Es benötigt dafür entsprechende Werkzeuge, die diese Datei bereitstellt.

Meiner datenschutzrechtlichen Bewertung sind dann Grenzen gesetzt, wenn sich ein Dateisystem aufgrund der stetigen Anpassungen nur sehr generisch beschreiben lässt. Der mir vom Bundesverfassungsgericht zugewiesenen Kontroll- und Kompensationsfunktion kann ich nur gerecht werden, wenn ich die Datei sowie die konkrete Nutzung regelmäßig kontrolliere und so anhand der Nutzungspraxis das Verständnis intensiviere. So kann mein Haus auch besser hinsichtlich datenschutzfreundlicher Fortentwicklungen beraten. Eine Kontrolle dieser Datei ist daher für das kommende Berichtsjahr geplant.

Auch wenn ich den Bedarf der Nachrichtendienste an solchen Systemen nicht in Abrede stelle, fehlt es für diese automatisierte Datenanalyse an einer ausreichenden Rechtsgrundlage. Denn diese Datenverarbeitung greift in das Recht auf informationelle Selbstbestimmung derjenigen ein, deren Daten im Zuge der Analyse personenbezogen genutzt werden. Gerade die zweckverändernde und zusammenführende Nutzung vormals getrennter Daten sowie darüber hinaus die Erlangung neuer Erkenntnisse aus der automatisierten Analyse begründen neue Grundrechtseingriffe. Für diese ist eine eigenständige Rechtsgrundlage erforderlich. Die Generalklausel des § 8 Abs. 1 BVerfSchG, auf die das BfV den Einsatz solcher Analysesysteme bisher stützt, stellt jedenfalls keine ausreichende Rechtsgrundlage dar, da dort keine Rahmenbedingungen geregelt sind.

**Kontrolle NADIS beim MAD**

Meine Mitarbeiterinnen und Mitarbeitern haben die bereits im vergangenen Berichtsjahr begonnene Kontrolle der Nutzung des Nachrichtendienstlichen Informationssystems (NADIS) beim Militärischen Abschirmdienst (MAD) abgeschlossen. Die grundlegenden Regelungen zur Teilnahme an NADIS und dessen Nutzung durch den MAD sind in § 6 BVerfSchG festgelegt.

**Wesentliche Regelungen aus § 6 BVerfSchG**

Der MAD darf am nachrichtendienstlichen Informationssystem teilnehmen, sofern die Verarbeitung personenbezogener Daten zur Erfüllung seiner gesetzlichen Aufgaben erforderlich ist. Die Vorschrift regelt insbesondere:

- Voraussetzungen für die Teilnahme am NADIS,
- zulässige Arten der Datenübermittlung,
- die Pflicht zur Sicherstellung eines angemessenen Datenschutzniveaus,
- Dokumentations- und Protokollanforderungen.

Ergänzend hierzu bestehen interne Dienstvorschriften des MAD, die den praktischen Einsatz von NADIS detailliert regeln. Gegenstand der Kontrolle war die Einhaltung dieser gesetzlichen und internen Vorgaben.

Verstöße gegen die maßgeblichen Bestimmungen oder sonstige schwerwiegende datenschutzrechtliche Defizite

haben meine Mitarbeiterinnen und Mitarbeitern nicht festgestellt. Es wurden jedoch mehrere praxisorientierte Empfehlungen ausgesprochen. Diese betreffen insbesondere die weitere Präzisierung und Vereinheitlichung der Dokumentation von Zugriffen auf NADIS. Ebenso wurden Empfehlungen allgemeiner Natur ausgesprochen, die das bereits hohe Datenschutzniveau beim MAD weiter ausbauen sollen. Ich begrüße ausdrücklich die Bereitschaft des MAD, diese Hinweise in seine organisatorischen Abläufe einzubeziehen.

Parallel zu den Kontrollen wurde auch die geplante Einführung neuer Systeme beim MAD begleitet. Hierzu zählen insbesondere Systeme, deren Komponenten teilweise KI basiert arbeiten sollen. Ich begrüße die frühzeitige Kontaktaufnahme durch den MAD ausdrücklich, da eine datenschutzrechtliche Beratung in frühen Projektphasen maßgeblich dazu beiträgt, Systeme zugleich praxisgerecht und datenschutzkonform zu gestalten. Frühzeitige Beteiligung ermöglicht es, potenzielle Risiken rechtzeitig zu erkennen, technische und organisatorische Schutzmaßnahmen angemessen auszuwählen und notwendige Anpassungen vorzunehmen, bevor die Systeme in die operative Umsetzung gehen.

**Kontrolle der Auslandsübermittlungen beim BfV und beim MAD**

Mit dem Gesetz zum ersten Teil der Reform des Nachrichtendienstrechts vom 22. Dezember 2023 wurden die Übermittlungs- und Protokollierungsvorschriften im Bereich der Nachrichtendienste reformiert. Dies hat mein Haus zum Anlass genommen, die Übermittlungen des MAD und des BfV an ausländische sowie über- und zwischenstaatliche Stellen gemäß § 25a BVerfSchG (beim MAD i. V. m. § 11 MADG) zu kontrollieren. Die Kontrolle beim MAD hat keine wesentlichen datenschutzrechtlichen Defizite ergeben, insbesondere sind sämtliche geprüften Übermittlungen rechtmäßig erfolgt.

Mein Haus hat allerdings angeregt, die Umsetzung eines abteilungsübergreifenden Handbuchs des MAD zu den rechtlichen Voraussetzungen der Übermittlungsvorschriften sowie zur Dokumentation und Protokollierung zu prüfen. Ein solches Vorgehen erleichtert ein einheitliches Verwaltungshandeln und trägt damit dazu bei, mögliche datenschutzrechtliche Defizite zu verhindern bzw. zu verringern. Zudem hat mein Haus darauf hingewiesen, dass nach § 25a Abs. 3 BVerfSchG auch dann ein Hinweis an den Empfänger der Daten erfolgen muss, wenn eine Übermittlung personenbezogener Daten nur mündlich erfolgt ist. Der sog. Empfängerhinweis bedeutet, dass der MAD die empfangende Stelle darauf hinweisen muss, welchen rechtlichen Beschränkungen die weitere Verwendung der Daten aufgrund Bundesrechts unterliegt. Dies ist eine der Anforderungen aus der verfassungsgerichtlichen Rechtsprechung, die der Gesetzgeber 2023 in die Nachrichtendienstgesetze aufgenommen hat.[58]

Da die Kontrolle des BfV zum Zeitpunkt des Redaktionsschlusses noch nicht abgeschlossen ist, werde ich hierzu im nächsten Tätigkeitsbericht ausführen.

## 7.10 Datenschutzrechtliche Kontrolle der ZITiS

**Erstmalige datenschutzrechtliche Kontrolle der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) durch meine Behörde.**

Die ZITiS unterstützt Sicherheitsbehörden des Bundes mit technischen Entwicklungen und Forschung in Bereichen wie Telekommunikationsüberwachung, Kryptoanalyse und digitaler Forensik. Aufgrund der zahlreichen möglichen Berührungspunkte mit personenbezogenen Daten kommt auch der datenschutzrechtlichen Kontrolle ihrer Tätigkeiten Bedeutung zu.

Im Berichtsjahr hat mein Haus eine erste datenschutzrechtliche Kontrolle bei der ZITiS eingeleitet, die im kommenden Jahr abgeschlossen wird. Aus Geheimschutzgründen kann ich an dieser Stelle auf keine Details eingehen.

Unabhängig vom Ausgang der Prüfung bestehen weiterhin offene Fragen zu gesetzlichen Aufgaben und Befugnissen der ZITiS. Soweit die ZITiS personenbezogene Daten verarbeitet oder künftig verarbeiten will, wäre hierfür eine ausdrückliche gesetzliche Grundlage erforderlich. Ein entsprechender Gesetzesentwurf wurde in der vergangenen Legislaturperiode nicht verabschiedet.

Mit entsprechenden Rechtsgrundlagen könnte die ZITiS einen noch umfassenderen Beitrag zur digitalen Souveränität und effektiveren Wahrnehmung der wichtigen Aufgaben der Sicherheitsbehörden leisten. Hierdurch würde Rechtssicherheit nicht nur für die ZITiS selbst, sondern auch für die Sicherheitsbehörden als Bedarfsträger gewährleistet.



58 Vgl. 32. TB Nr. 3.3.1

## 7.11 Kontrollen und Qualifizierung im Anwendungsbereich des SÜG

**Durch Kontrolle, Beratung und Qualifizierung wird der Datenschutz im SÜG-Bereich kontinuierlich und nachhaltig verbessert. Hierzu haben meine Mitarbeiterinnen und Mitarbeiter im Berichtsjahr 22 Kontrollen durchgeführt, diverse Vorträge gehalten sowie Schulungsangebote weiter ausgebaut.**

Im Berichtsjahr habe ich im Anwendungsbereich des Sicherheitsüberprüfungsgesetzes (SÜG) zwölf öffentliche Stellen und zehn Unternehmen kontrolliert.[59] Die Kontrollen zeigten erneut, dass sich bestimmte Problemfelder im Bereich der Sicherheitsüberprüfung hartnäckig halten.[60] Die häufigsten Feststellungen betrafen Verstöße gegen gesetzliche Vernichtungs- und Löschfristen, eine unzureichende Personalausstattung im Geheim- und Sabotageschutzbereich sowie die unzulässige Einbindung von Sicherheitsbevollmächtigten und Sabotageschutzbeauftragten von Fremdfirmen in die Abwicklung der Sicherheitsüberprüfung. Aufgrund dieser strukturellen Defizite konnte bei den betroffenen Stellen ein risikoangemessenes Schutzniveau für die im Rahmen des SÜG verarbeiteten personenbezogenen Daten nicht gewährleistet werden.

Positiv hervorzuheben ist demgegenüber, dass beispielsweise die in den Vorjahren durchgeführten Kontrollen bei den Bundespolizeidirektionen spürbar Wirkung gezeigt haben. Die in diesem Berichtsjahr kontrollierte Bundespolizeidirektion München setzte die datenschutzrechtlichen Anforderungen im SÜG nunmehr überwiegend ordnungsgemäß um.

Um diese Entwicklungen zu fördern, den Wissenstransfer weiter zu stärken und Fehler im Voraus zu vermeiden, wurden die Dialog- und Schulungsangebote weiter ausgebaut. Insbesondere habe ich im Berichtsjahr zwei mehrtägige Veranstaltungen für Teilnehmende der gesamten Bundesverwaltung angeboten, die stark nachgefragt wurden und fortgesetzt werden sollen.

Die Erfahrungen des Berichtsjahres zeigen deutlich, dass regelmäßige Kontrollen, kontinuierliche Beratungen, die Bereitstellung von Arbeitshilfen und der fachliche Austausch zwischen den beteiligten Stellen entscheidende Instrumente sind, um den Datenschutz im sensiblen Bereich der Sicherheitsüberprüfung nachhaltig zu stärken.



59 Übersicht der kontrollierten Stellen unter: www.bfdi.bund.de/tb-34-kontrollen
60 Vgl. 33. TB Nr. 7.4.5, 32. TB Nr. 9.1.6

# 8 Gremienarbeit

## 8.1 Bericht aus dem EDSA

**Der Europäische Datenschutzausschuss (EDSA) hat im Berichtsjahr seine Arbeit an einer europaweit harmonisierten Anwendung der Datenschutz-Grundverordnung (DSGVO) kontinuierlich fortgesetzt. Einen weiteren Schwerpunkt stellte die Umsetzung der Europäischen Datenstrategie und des Pakets für digitale Dienste dar. Hier hat der EDSA Leitlinien zu Wechselwirkungen der neuen Rechtsakte mit der DSGVO angenommen.**

Im Jahr 2025 hat der EDSA insgesamt 12-mal konferiert. Hinzu kamen zahlreiche Sitzungen der 14 Arbeitsgruppen (Expert Subgroups), zweier Task Forces und des Coordinated Supervision Committees (CSC) mit seinen Arbeitsgruppen (Working Groups), an deren Arbeiten sich meine Mitarbeiterinnen und Mitarbeiter aktiv beteiligt haben.

Der EDSA hat im Berichtsjahr auf Anforderung der Europäischen Kommission (EU-Kommission) mehrere Stellungnahmen nach Art. 70 Abs. 1 Buchst. s DSGVO zu **Adäquanzbeschlüssen** abgegeben. Diese betreffen das Vereinigte Königreich und Brasilien sowie mit der Europäischen Patentorganisation erstmals eine zwischenstaatliche Organisation[61].

Gemeinsam mit dem Europäischen Datenschutzbeauftragten (EDSB) hat der EDSA eine Stellungnahme[62] nach Art. 42 Abs. 2 der Verordnung (EU) 2018/1725 zum Entwurf der EU-Kommission für eine Verordnung im Hinblick auf die Ausweitung bestimmter Risikominderungsmaßnahmen, die kleinen und mittleren Unternehmen (KMU) zur Verfügung stehen, veröffentlicht (sog. Omnibus IV)[63]. Der EDSA und der EDSB unterstützten darin die Zielsetzung der EU-Kommission, die bürokratischen Anforderungen für KMU und kleine „Mid-Cap"-Unternehmen (SMC) zu reduzieren.

Im **Kohärenzverfahren** nach Art. 64 Abs. 1 DSGVO hat der EDSA im Berichtsjahr 22 Stellungnahmen abgegeben[64]. Diese betreffen durch Datenschutzaufsichtsbehörden der Mitgliedstaaten vorgelegte verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO), die Akkreditierung von Zertifizierungsstellen (Art. 43 Abs. 3 DSGVO) und die Akkreditierung von Stellen zur Überwachung der Einhaltung von Verhaltensregeln (Art. 41 DSGVO).

Der EDSA hat im Berichtsjahr fünf **Leitlinien** verabschiedet[65], u. a. zur **Pseudonymisierung** sowie zur Verarbeitung personenbezogener Daten mittels **Blockchain-Technologie**. Zwei weitere Leitlinien betreffen die Wechselwirkung **(„Interplay")** zwischen dem **Digital Services Act (DSA)** und der DSGVO sowie zwischen dem **Digital Markets Act (DMA)** und der DSGVO. Zudem hat er Empfehlungen zur Umsetzung der Fluggastdaten-Richtlinie ausgesprochen.[66]

Mit der sog. **Helsinki-Erklärung** („The Helsinki Statement on enhanced clarity, support and engagement")[67] hat der EDSA Maßnahmen zur Vereinfachung und größeren Effizienz seiner Arbeiten beschlossen, die insbesondere KMU die Einhaltung der DSGVO in der Praxis erleichtern sollen. Der EDSA beabsichtigt, den Dialog mit den Interessengruppen zu verstärken, indem diese proaktiver und frühzeitiger beteiligt werden.

61 https://www.edpb.europa.eu/our-work-tools/consistency-findings/opinions_en?f%5B0%5D=opinions_topics%3A110
62 EDPB-EDPS Joint Opinion 01/2025 on the Proposal for a Regulation on simplification measures for SMEs and SMCs, in particular the record-keeping obligation under Art. 30(5) GDPR
63 COM(2025)501 – Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573
64 https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en
65 https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en
66 https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-22025-implementation-pnr-directive-light-cjeu_en
67 https://www.edpb.europa.eu/our-work-tools/our-documents/statements/helsinki-statement-enhanced-clarity-support-and-engagement_en

Gemeinsam mit den Aufsichtsbehörden der Länder setze ich mich aktiv für die Umsetzung der Helsinki-Erklärung ein, um Grundrechte der Bürgerinnen und Bürger zu schützen und datenschutzfreundliche Technologien sowie Innovationen innerhalb eines kohärenten Rahmens von Digitalgesetzgebung und Datenschutzrecht zu fördern.

**Zur Liste der Gremien**

(QR-Code klicken oder scannen)

## 8.2 Die neue CIC ESG

**Im Berichtsjahr hat der EDSA seine Taskforce zum Zusammenspiel zwischen Datenschutz, Wettbewerb und Verbraucherschutz[68] verstetigt zur neuen Arbeitsgruppe für regulierungsübergreifendes Zusammenspiel und behördliche Zusammenarbeit, der „Cross-Regulatory Interplay and Cooperation" Expert Subgroup (CIC ESG).**

Die neue CIC ESG soll dazu beitragen, die Verbindungen zwischen den Rechtsrahmen für Datenschutz, Wettbewerb und Verbraucherschutz zu klären. Zudem soll sie bewährte Verfahren für behördenübergreifende Governance und Zusammenarbeit fördern, insbesondere im Zusammenhang mit der Ausführung der EU-Digitalgesetzgebung.

Hierzu veröffentlichte der EDSA beispielsweise ein unter Co-Federführung meiner Behörde erstelltes Positionspapier der CIC ESG zu dem Zusammenspiel zwischen Datenschutz- und Wettbewerbsrecht[69]. Ebenfalls unter Co-Federführung meiner Behörde wurde eine Übersicht über den Stand der Umsetzung mehrerer EU-Digitalrechtsakte und der diesbezüglichen neuen Befugnisse von Datenschutzaufsichtsbehörden in den EU-Mitgliedstaaten erstellt.

Weiterhin unterstützt die CIC ESG die Hochrangige Gruppe zum Digitale-Märkte-Gesetz (DMA) der EU. Das Beratungsgremium behandelt die Themen Künstliche Intelligenz, Interoperabilität von Messengerdiensten und sonstige datenbezogene Vorschriften im DMA. Im Berichtsjahr verabschiedete das Beratungsgremium eine Stellungnahme zur Künstlichen Intelligenz, in der eine engere behördenübergreifende Zusammenarbeit im Hinblick auf den Einsatz von KI-Systemen durch designierte Unternehmen, die zentrale Plattformdienste anbieten (sog. Torwächter), vorgeschlagen wird.

## 8.3 Internationale Datenübermittlungen – Angemessenheit des Rechtsrahmens

**Im Juli 2025 erließ die Europäische Kommission (EU-Kommission) für die Europäische Patentorganisation den ersten Angemessenheitsbeschluss für eine Internationale Organisation. Ende des Jahres folgten zwei Angemessenheitsbeschlüsse für das Vereinigte Königreich (VK). Zudem hat die EU-Kommission den Angemessenheitsbeschluss für Brasilien für den Erlass zum Jahresbeginn 2026 vorbereitet. Mein Haus war maßgeblich an den Stellungnahmen des Europäischen Datenschutzausschusses für die Verfahren zur Verabschiedung dieser beteiligt.**

### Zwei neue Angemessenheitsbeschlüsse für das Vereinigte Königreich (VK)

Am 19. Dezember 2025 erließ die EU-Kommission zwei neue Angemessenheitsbeschlüsse für das Vereinigte Königreich, durch die sowohl für Datenübermittlungen nach der Datenschutz-Grundverordnung (DSGVO) als auch nach der Strafverfolgungsrichtlinie (JI-Richtlinie) ein angemessenes Schutzniveau jeweils festgestellt wird[70]. Das Vereinigte Königreich ist weiterhin das einzige Drittland, für das bislang ein Beschluss nach der JI-Richtlinie verabschiedet wurde.

Die in Folge des Brexit ursprünglich im Jahr 2021 in Kraft getretenen Angemessenheitsentscheidungen waren bis zum 27. Juni 2025 befristet. Aufgrund des im VK im Frühsommer noch andauernden Gesetzgebungsverfahrens zum sog. Data Use and Access Act (DUA Act)[71] entschloss sich die Europäische Kommission, beide Angemessenheitsbeschlüsse zunächst um ein halbes



68 Vgl. 33. TB Nr. 4.2.1
69 https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/position-paper-interplay-between-data-protection-and_en
70 Verlängerung des Angemessenheitsbeschlüsse für UK: https://commission.europa.eu/document/a7907f8f-6e1c-4782-a193-d16b2cfe7650_en (DSGVO) und https://commission.europa.eu/document/fcb17e2f-40a5-46ed-8435-7a76434d19fb_en (JI-RL)
71 https://www.legislation.gov.uk/ukpga/2025/18/contents

Jahr bis zum 27. Dezember 2025 zu verlängern[72]. Das Verfahren zur Annahme der neuen Angemessenheitsbeschlüsse startete die EU-Kommission Ende Juli 2025 nach Inkrafttreten des DUA Acts durch die Übermittlung der Entwürfe zwecks Stellungnahmen des EDSA.

Beide Angemessenheitsbeschlüsse enthalten erneut ein „Ablaufdatum", und zwar zum 27. Dezember 2031. Damit sind sie die einzigen Angemessenheitsbeschlüsse mit einer festen zeitlichen Begrenzung.

Grundsätzlich begrüßen beide Stellungnahmen des EDSA[73] zu den Entwürfen der Angemessenheitsbeschlüsse den fortbestehenden Gleichlauf zwischen dem Datenschutzrahmen des VK und dem der EU. Der EDSA regt gegenüber der EU-Kommission allerdings an, verschiedene rechtliche Änderungen im VK im Rahmen ihrer Angemessenheitsbewertung genauer zu untersuchen. Hier sind etwa erweiterte Ausnahmeregelungen zu nennen, nach denen Strafverfolgungsbehörden Datenschutzvorschriften zum Schutz der nationalen Sicherheit unangewendet lassen können. Zudem erhält der zuständige Minister nach den Änderungen durch den DUA Act neue Befugnisse[74], nach denen er bestimmte Bereiche spezifischer regeln kann, ohne das Parlament zu beteiligen. Schließlich ändert sich auch die Struktur der Aufsicht.

**Brasilien**

Die EU-Kommission hat im September 2025 den Entwurf für einen Angemessenheitsbeschluss für Brasilien veröffentlicht.[75] In der im November beschlossenen Stellungnahme[76] stellte der EDSA positiv fest, dass der brasilianische Datenschutzrahmen eng an die Datenschutzanforderungen der DSGVO und die Rechtsprechung des EuGH angelehnt ist. Dies gilt insbesondere in Bezug auf die Rechte betroffener Personen, internationale Übermittlungen, die Aufsicht, Rechtsbehelfe und den Bereich „Government Access" (bspw. durch Strafverfolgungsbehörden), für den eine weitgehende Bereichsausnahme gilt.

Insoweit sind nur die im brasilianischen Recht kodifizierten Datenschutzgrundsätze anwendbar. Weitergehende Kodifikationen, die den Bereich des „Government Access" spezifisch regeln, finden sich nur in begrenztem Umfang. Vor diesem Hintergrund gab der EDSA der EU-Kommission für diesen Bereich auf, die Fortentwicklungen zu überwachen.

**Europäische Patentorganisation (EPO)**

Besonders hervorheben möchte ich, dass zum 15. Juli 2025 erstmals für eine Internationale Organisation – die Europäische Patentorganisation (EPO) – ein Angemessenheitsbeschluss gefasst wurde[77].

Die EPO ist keine Institution der EU, sondern eine zwischenstaatliche Organisation, deren Aufgabe es ist, das Europäische Patentübereinkommen umzusetzen. Patente sind wissenschaftlich wie wirtschaftlich von hoher Bedeutung, weshalb der Schutz der Anträge und der in ihnen enthaltenen personenbezogenen Daten entsprechend sensibel ist.

Mit diesem Angemessenheitsbeschluss bescheinigt die Europäische Kommission, dass der Datenschutzrahmen der EPO ein im Wesentlichen gleichwertiges Datenschutzniveau im Verhältnis zur DSGVO gewährleistet. Damit zeigt sie auf, dass die Bestimmungen der DSGVO zu internationalen Datenübermittlungen einen sicheren Datenfluss aus der EU/dem EWR zu internationalen Organisationen unter Berücksichtigung ihres besonderen Status ermöglichen können.

**Aktuelle Entwicklungen zum EU-U.S. Data Privacy Framework**

Bereits kurz nach Inkrafttreten des Angemessenheitsbeschlusses für die USA hatte der französische Abgeordnete des Europäischen Parlaments, Herr Philippe Latombe, Nichtigkeitsklage gegen den Beschluss erhoben. In der Rechtssache Latombe ./. EU-Kommission hat das Gericht der Europäischen Union den Beschluss in erster Instanz

72 06/2025, Stellungnahme des EDSA zur Verlängerung der beiden Angemessenheitsbeschlüsse für UK: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-062025-regarding-extension-european-commission_en

73 26/2025 Stellungnahme des EDSA zum Entwurf eines Angemessenheitsbeschlusses zur DSGVO: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-262025-regarding-european-commission-draft_en
27/2025 Stellungnahme des EDSA zum Entwurf eines Angemessenheitsbeschlusses zur JI-RL: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-272025-regarding-european-commission-draft_en

74 Abschnitt 1.4.2, S. 10, 26/2025 Stellungnahme des EDSA: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-262025-regarding-european-commission-draft_en

75 Entwurf des Angemessenheitsbeschlusses für Brasilien: https://commission.europa.eu/document/f5aee532-70bf-41b1-a94a-8e294a528f6a_en

76 Stellungnahme zum Entwurf eines Beschlusses der Europäischen Kommission über ein angemessenes Schutzniveau für personenbezogene Daten in Brasilien, angenommen am 4. November 2025, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282025-regarding-european-commission-draft_en

77 Angemessenheitsbeschluss der Europäischen Kommission für die Europäische Patentorganisation: https://commission.europa.eu/document/download/2687dc39-5217-4165-8db6-b1294dc5b591_en?filename=EPO%20Adequacy%20Decision%20July%202025.pdf

bestätigt. Das EU-U.S. Data Privacy Framework bleibt damit weiterhin eine gültige Grundlage für Datenübermittlungen in die USA. Abschließende Rechtssicherheit bietet das erstinstanzliche Urteil jedoch nicht. Bevor es rechtskräftig wurde, legte der Kläger Rechtsmittel beim Europäischen Gerichtshof (EuGH) ein. Damit steht eine endgültige Entscheidung über diese Klage zum EU-U.S. Data Privacy Framework noch aus. Diese kann weitreichende Auswirkungen auf die Praxis der Drittstaatenübermittlungen haben.

## 8.4 Experten-Workshop zu DSGVO-Zertifizierung

**Erfahrungsaustausch und Prozessverbesserung bei Zertifizierungsverfahren nach Art. 42 DSGVO standen bei einem Workshop von Datenschutzaufsichtsbehörden und weiteren Stakeholdern im Fokus.**

Im Juni 2025 veranstalteten die deutschen Datenschutzaufsichtsbehörden im Rahmen einer Expertengruppe des Europäischen Datenschutzausschusses (EDSA) einen dreitägigen Workshop zum Thema Zertifizierungsverfahren nach Art. 42 Datenschutz-Grundverordnung (DSGVO). Aus der ganzen EU kamen Expertinnen und Experten in meinem Verbindungsbüro in Berlin zusammen und diskutierten, wie DSGVO-Zertifizierung genutzt werden kann, um das Datenschutzniveau europaweit zu verbessern.

Die DSGVO sieht die Förderung von datenschutzspezifischen Prüfverfahren und Datenschutzsiegeln vor, die nachweisen sollen, dass die DSGVO bei Verarbeitungsvorgängen eingehalten wird. In diesem Kontext ist vorgesehen, dass Zertifizierungskriterien ein Genehmigungsverfahren im EDSA durchlaufen.

Die zuständige Expertengruppe evaluierte gemeinsam mit Vertreterinnen und Vertretern von Zertifizierungs-, Akkreditierungsstellen und Programmeignern, wie Prozesse rund um die Zertifizierung verbessert werden können und welche Erfahrungen bereits gemacht wurden. Alle beteiligten Akteurinnen und Akteure waren sich einig, dass die Zertifizierung ein erhebliches Potenzial bietet, von dem betroffene Personen, Unternehmen, Zertifizierungsstellen und auch Datenschutzaufsichtsbehörden profitieren können.

## 8.5 DSK-Merkblatt zu Verständigungen

**Die Datenschutzkonferenz (DSK) hat ein gemeinsames Merkblatt zu Verständigungen in datenschutzrechtlichen Verfahren über Geldbußen bereitgestellt.**

In ihrer letzten Sitzung des Jahres 2025 hat die DSK ein Merkblatt zu Verständigungen in datenschutzrechtlichen Verfahren über Geldbußen angenommen. Es gilt für nationale Verfahren und findet keine Anwendung auf grenzüberschreitende Verfahren. Das Merkblatt erläutert, auf welcher rechtlichen Grundlage Verständigungen erfolgen, und zeigt die rechtsstaatlichen Rahmenbedingungen auf. Es macht transparent, wie Verständigungsgespräche mit den Datenschutzaufsichtsbehörden ablaufen und welche Bedingungen sie für eine Verständigung stellen. Im Ergebnis ermöglicht das Merkblatt Stellen, die bereit sind, sich einsichtig und geständig zu zeigen, eine angemessene Minderung der Geldbuße zu erreichen. Das Merkblatt wurde durch die DSK veröffentlicht.[78]

## 8.6 Einigung zu DSK-Musterrichtlinien

**Die Datenschutzkonferenz (DSK) hat Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden angenommen.**

In ihrer Sitzung am 16. Juni 2025 hat sich die DSK auf Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden verständigt. Die Musterrichtlinien wurden durch die DSK veröffentlicht.[79] Sie enthalten wichtige verfahrensrechtliche Klarstellungen im Zusammenspiel zwischen DSGVO und dem Gesetz über Ordnungswidrigkeiten (OWiG). Sie machen transparent, wie die Datenschutzaufsichtsbehörden die Vorgaben aus Urteilen des EuGH verfahrensrechtlich behandeln. Die Behördenleitungen der Datenschutzaufsichtsbehörden des Bundes und der Länder, soweit diese für den nicht-öffentlichen Bereich zuständig sind, beabsichtigen, die Musterrichtlinien in ihrer Behörde jeweils als Verwaltungsvorschriften zu erlassen.



78 Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/DSK_Merkblatt_Verstaendigung.pdf
79 Siehe hierzu: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/DSK-Festlegung_MRiDaVG.pdf

# 9 Informationsfreiheit

## 9.1 Überblick in Zahlen

**Eingaben mit Bezug zum Informationsfreiheitsgesetz (IFG) und zum Umweltinformationsgesetz (UIG)**

Im Bereich Informationsfreiheit erreichten mich im Berichtsjahr insgesamt 538 Eingaben. In 356 Fällen riefen mich Petenten nach § 12 Abs. 1 IFG an und rügten eine Verletzung ihres Rechts auf Informationszugang nach dem IFG. Mit der Bitte um Vermittlung bei Anträgen nach dem UIG wandten sich antragstellende Personen in 30 Fällen an mich (§ 7a UIG). Im Vergleich zum Vorjahr stieg die Zahl der Vermittlungsbitten hinsichtlich der Anträge nach dem UIG damit abermals leicht.

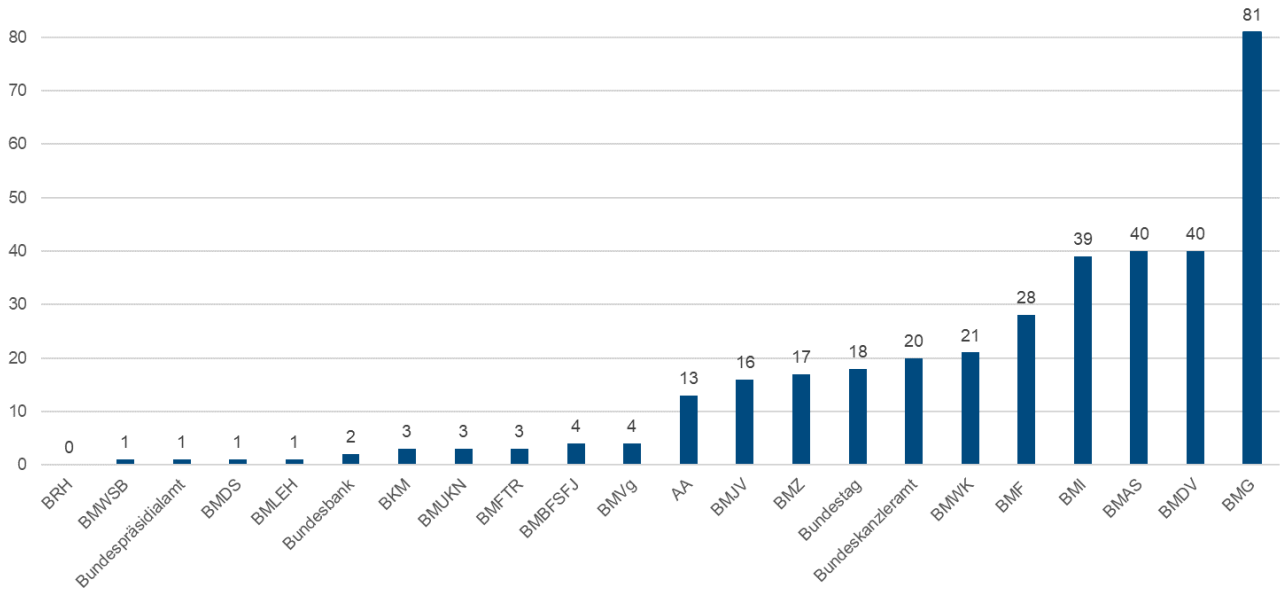
Neben den Anrufungen wegen einer Verletzung des Rechts auf Informationszugang wurden im Berichtsjahr auch 36 allgemeine Anfragen gestellt, in denen es um Rechtsauskünfte zum IFG ging, um Bürgeranfragen oder um Vermittlungsbegehren außerhalb meiner Zuständigkeit.

Bezogen auf die Ressorts und ihre Geschäftsbereiche verteilen sich die Anrufungen nach § 12 Abs. 1 IFG wie aus der nachfolgenden Grafik ersichtlich. Die höchste Zahl betraf wie in den Vorjahren das Bundesministerium für Gesundheit (BMG) und seinen Geschäftsbereich.

**IFG-Anträge an meine Behörde**

Im Berichtsjahr gingen insgesamt 116 Anträge auf Informationszugang bei mir ein. Diese Anträge richteten sich sowohl auf den Zugang zu Akteninhalten im Rahmen von eigenen, an meine Behörde gerichteten Vermittlungsbitten nach deren Abschluss als auch auf meine Stellungnahmen zu Gesetzesvorhaben. Im Vergleich zu den Vorjahren ist das Antragsaufkommen gleichbleibend.

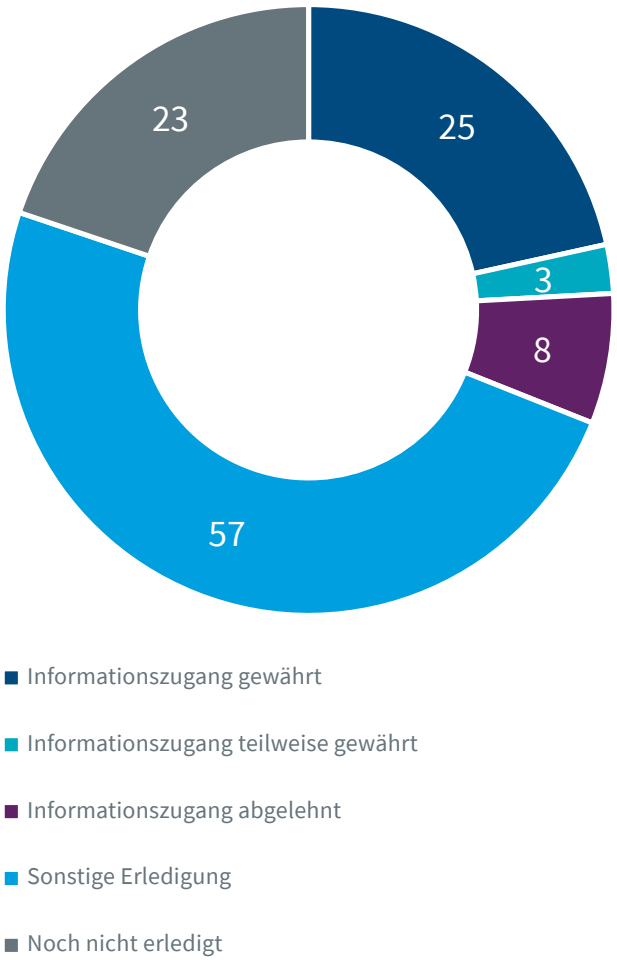
**Anrufungen nach § 12 IFG im Berichtsjahr nach Ressorts**



Aus der Abbildung ergibt sich die Verteilung der (teilweisen) Zugangsgewährung, der Zugangsablehnung und der sonstigen Erledigung im Jahr 2025. Fälle der sonstigen Erledigung umfassen bspw. Vorgänge, bei denen der Antrag wegen voraussichtlicher Gebührenpflichtigkeit nicht weiterverfolgt wurde oder Vorgänge, bei denen der Antragsteller nicht hinreichend mitgewirkt hat.

Gründe für Ablehnungen waren im Wesentlichen andauernde Beratungen oder die Tatsache, dass die erbetenen Informationen in meinem Haus nicht vorliegen.

**IFG-Anträge an meine Behörde im Berichtsjahr**




## 9.2 Beratungen und Kontrollen

**Im Bereich der Informationsfreiheit fanden im Berichtsjahr diverse Fachformate zur Abstimmung, Beratung, Kontrolle und zum Austausch statt.**

**Beratungs- und Kontrollbesuch beim BMF**

Im Juni 2025 wurde der Kontrollbericht über den Beratungs- und Kontrollbesuch zur Informationsfreiheit beim Bundesministerium der Finanzen (BMF) veröffentlicht. Der Besuch selbst fand bereits Ende 2024 statt und hatte die Bearbeitung von Anträgen nach dem Informationsfreiheitsgesetz (IFG) und dem Umweltinformationsgesetz (UIG) zum Gegenstand.

Für die Prüfung wurden 172 von insgesamt rund 1.350 IFG- und UIG-Vorgängen aus dem Zeitraum 2020 bis 2024 durchgesehen und bewertet. Das zentrale Ergebnis des Besuchs ist positiv: Die Anwendung des IFG und UIG im BMF erfolgt bürger- und serviceorientiert. Verfahrensvorschriften und materiell-rechtliche Vorgaben werden – bis auf wenige Ausnahmen – durchgehend beachtet.

**Beratungs- und Kontrollbesuch im AA**

Im November 2025 wurde ein Beratungs- und Kontrollbesuch beim Auswärtigen Amt (AA) durchgeführt. Gegenstand der Prüfung war die Bearbeitung von Anträgen nach dem Informationsfreiheitsgesetz (IFG) und dem Umweltinformationsgesetz (UIG).

Die Überprüfung basierte auf der Auswertung von 175 von insgesamt circa 1.800 IFG-Vorgängen aus dem Zeitraum 2022 bis 2025. Das Fazit des Besuchs ist positiv: Im Auswärtigen Amt herrscht eine ausgeprägt offene und positive Haltung gegenüber der Informationsfreiheit. Die Anwendung des IFG und UIG erfolgt sehr bürger- und serviceorientiert. Verfahrens- und materiell-rechtliche Vorgaben werden – abgesehen von wenigen Einzelfällen – durchgehend beachtet.

**Erfahrungsaustausch der Bundesbehörden zur Informationsfreiheit**

Einen etablierten Teil meines Beratungsangebotes stellen die beiden Erfahrungsaustausche mit den obersten Bundesbehörden in Berlin und mit verschiedenen Bundesoberbehörden und -anstalten in Bonn dar. Hierbei haben alle Teilnehmenden die Möglichkeit, sich über allgemeine Fragen der Bearbeitungspraxis von Informationsfreiheitsanträgen auszutauschen. Auch in diesem Berichtsjahr wurden diese Formate wieder an mehreren Terminen mit Erfolg durchgeführt.

**Workshop mit der Techniker Krankenkasse**

Im Mai 2025 habe ich mit der Techniker Krankenkasse (TK) einen Workshop zu der Bearbeitung von Anträgen nach IFG und UIG durchgeführt. Anlass dafür war die dortige Neuorganisation der Antragsbearbeitung. Im Rahmen dieses neuen, auf maßgeschneiderte Be-

ratungslösungen ausgelegten Formats habe ich der TK Hinweise, Anregungen und Empfehlungen zu der konkreten Ausgestaltung einer rechtskonformen und effizienten wie auch bürgerfreundlichen Bearbeitungspraxis gegeben.

## 9.3 Gremienarbeit

**16. Internationale Konferenz der Informationsfreiheitsbeauftragten 2025**

**Vom 23. bis 25. Juni 2025 veranstaltete die BfDI die 16. Internationale Konferenz der Informationsfreiheitsbeauftragten (ICIC) in Berlin. Die ICIC ist die weltweite Konferenz der Aufsichtsbehörden im Bereich der Informationsfreiheit. An der Konferenz nahmen über 140 internationale Gäste aus 60 Mitgliedstaaten teil.**

Vertreterinnen und Vertreter aus Wissenschaft, Medien, Zivilgesellschaft und mehr als 50 Informationsfreiheitsbeauftragte aus aller Welt diskutierten unter dem Titel „Access to Environmental Information in a Digital Era“ über rechtliche Fragen und praktische Perspektiven der Informationsfreiheit.

Thematisiert wurde, wie der Zugang zu Umweltinformationen weltweit einfacher und wirksamer gestaltet werden kann und welche Potenziale digitale Technologien bieten, um eine proaktive und grenzüberschreitende Bereitstellung von Umwelt- und Klimadaten zu ermöglichen.

Die Schwerpunkte der Veranstaltung bildeten ein Vergleich internationaler rechtlicher Rahmenbedingungen, die Herausforderungen angesichts politischer Unsicherheiten, digitaler Transformation und wachsender Datenmengen sowie die Bedeutung des Zugangs zu Umweltinformationen für marginalisierte Gruppen und deren Teilhabe. Zudem wurde erörtert, wie zusammen mit Open-Data-Strategien die proaktive Veröffentlichung von Umweltinformationen gestärkt werden kann.

Die Konferenz spiegelte die Breite der aktuellen Debatten und verdeutlichte, dass das Recht auf Zugang zu Informationen ein entscheidendes Element für Transparenz, demokratische Teilhabe und nachhaltige Entwicklung bleibt.

Anlässlich der ICIC haben die europäischen Partner das European Network for Transparency and Right to Information (ENTRI) gegründet. Die BfDI hat den Vorsitz des neuen Netzwerks für die kommenden drei Jahre übernommen.

**ICIC 2025 Conference Report in englischer Sprache**

(QR-Code klicken oder scannen)

**Konferenz der Informationsfreiheitsbeauftragten**

Als Zusammenschluss der Beauftragten für Akteneinsicht, Informationsfreiheit und Transparenz des Bundes und der Länder widmet sich die Konferenz der Informationsfreiheitsbeauftragten (IFK) – unter jährlich wechselndem Vorsitz – der Förderung und Fortentwicklung staatlicher Transparenz in Bund und Ländern. Die IFK tagte unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit am 18. Juni 2025 in Jena und am 26. November 2025 in Erfurt. Beide Konferenzen wurden inhaltlich vom Arbeitskreis Informationsfreiheit (AKIF) vorbereitet.

**Dritter Europäischer Case Handling Workshop zur Informationsfreiheit**

Vom 7. bis 8. April 2025 fand der dritte Europäische Case Handling Workshop zur Informationsfreiheit in Pristina, Kosovo statt. Schwerpunktmäßig befasste sich der Case Handling Workshop mit Fällen im Zusammenhang mit Ausgaben öffentlicher Mittel sowie mit Fällen, bei denen Betriebs- und Geschäftsgeheimnisse oder der Schutz des geistigen Eigentums der Informationszugangsgewährung entgegenstanden.

## 9.4 Informationspflicht juristischer Personen des Privatrechts gemäß § 2 Abs. 1 Nr. 2 UIG

**Inwieweit auch private Unternehmen der Informationspflicht nach dem Umweltinformationsgesetz des Bundes (UIG) unterliegen, gewinnt vor dem Hintergrund wachsender staatlicher Beteiligungen an Privatunternehmen im Energie- und Umweltbereich zunehmend an praktischer Bedeutung. Hierbei stellen sich insbesondere Auslegungsfragen bezüglich des Tatbestandsmerkmals der „Kontrolle des Bundes“.**

Nach dem UIG können auch natürliche oder juristische Personen des Privatrechts informationspflichtige Stellen sein, soweit sie öffentliche Aufgaben mit Umweltbezug

wahrnehmen und der Kontrolle des Bundes unterliegen (§ 2 Abs. 1 Nr. 2 UIG). Eine Kontrolle in diesem Sinne wird unwiderleglich vermutet, wenn der Bund die Mehrheit des gezeichneten Kapitals eines Unternehmens besitzt (§ 2 Abs. 2 Nr. 2 Buchst. a UIG). Sinn und Zweck der Vorschriften ist es, einer fortschreitenden Verlagerung von staatlichen Aufgaben auf Private zu begegnen und eine „Flucht in das Privatrecht“ zu verhindern.

Gegenstand eines Vermittlungsverfahrens war die Frage, ob ein privatwirtschaftliches Unternehmen, das im Zusammenhang mit einer finanziellen Stabilisierungsmaßnahme vorübergehend unter staatlicher Kontrolle steht, der Informationspflicht nach dem UIG unterfällt. Ein Petent beantragte auf Grundlage des UIG bei einem Energieunternehmen den Zugang zu Informationen, die u. a. die Kohlendioxid-Emissionen von Dienstwagen betrafen. Mehrheitseigner des betroffenen Unternehmens ist der Bund. Es bestand hier allerdings die Besonderheit, dass dieser die Beteiligung im Rahmen von Stabilisierungsmaßnahmen nach dem Energiesicherungsgesetz (EnSiG) erworben hatte. Hierbei handelte es sich um eine von der EU-Kommission genehmigte, ausdrücklich vorübergehende Notfallmaßnahme zur Sicherung der bundesweiten Energieversorgung.

Das Unternehmen vertrat die Auffassung, dass es keine informationspflichtige Stelle im Sinne des UIG sei, und begründete dies insbesondere mit dem Sinn und Zweck der Erstreckung der Informationspflicht auf Private. Erfasst werden solle staatliches Handeln auch in privater Rechtsform. Im konkreten Fall gehe es jedoch um privatwirtschaftliches Handeln, das lediglich aus Gründen der Energiesicherung staatlich gestützt worden sei. Der Bund habe die Mehrheitsanteile nicht aufgrund eigener wirtschaftlicher Entscheidungen übernommen, sondern zwangsläufig und lediglich vorübergehend im Rahmen der erforderlichen Stabilisierungsmaßnahmen. Eine Einbeziehung des Unternehmens in den Anwendungsbereich des UIG sei entsprechend nicht mehr vom Sinn und Zweck der gesetzlichen Vorschriften gedeckt.

Dieser rechtlichen Einschätzung konnte ich mich nicht anschließen. Ich setzte das Unternehmen darüber in Kenntnis, dass die tatbestandlichen Voraussetzungen des § 2 Abs. 1 Nr. 2 UIG nach meiner Auffassung erfüllt seien. Insbesondere im Hinblick auf das Kriterium „staatlicher Kontrolle“ bieten weder der Wortlaut des UIG noch der zugrundeliegenden Umweltinformationsrichtlinie (RL 2003/4/EG[80]) einen Anhaltspunkt für das Erfordernis einer „Dauerhaftigkeit“ staatlicher Beherrschung. Auch eine Differenzierung hinsichtlich des Zwecks oder der Art und Weise einer Anteilsübernahme ist im Normtext nicht verankert. Ein engeres Normenverständnis, als es der eindeutige Gesetzeswortlaut vorgibt, dürfte deshalb eine teleologische Reduktion erfordern. Konkrete Anhaltspunkte, dass der Wortlaut der Vorschriften mit der gesetzgeberischen Intention und dem Gesetzeszweck nicht übereinstimmt, waren für mich jedoch nicht feststellbar.

Gleichwohl ist festzustellen, dass der Erwerb der staatlichen Beteiligung auf Grundlage einer nur vorübergehenden, streng zweckgebundenen Stabilisierungsmaßnahme eine besondere Fallkonstellation darstellt. Eine Rechtsverletzung war deshalb in den Grenzen des Vermittlungsverfahrens für mich nicht eindeutig feststellbar. Trotz meiner rechtlichen Hinweise hielt das Unternehmen an seiner Auffassung fest. Eine verbindliche Klärung der Rechtsfrage ist den Gerichten vorbehalten.

## 9.5 Die Flucht in den öffentlich-rechtlichen Dienstleister

**Wenn sich eine informationspflichtige Stelle zur Speicherung von E-Mails und anderen amtlichen Informationen eines öffentlich-rechtlichen Dienstleisters bedient, darf dies nicht dazu führen, dass die gespeicherten Nachrichten dem Informationszugang nach dem IFG entzogen sind.**

Mehrere Petenten wandten sich an mich, weil sie im Zusammenhang mit Recherchen zu der Cum-Ex-Affäre erfolglos Zugang zu E-Mail-Nachrichten eines ehemaligen Bundesministers beantragt hatten. Zunächst hatten sich die Petenten jeweils an das Ministerium gewandt. Dieses hatte die Anträge abgelehnt, weil die Informationen dort nicht (mehr) vorhanden seien. Erst im Nachhinein hatte das Ministerium dann erklärt, dass die betroffenen Postfächer noch existierten und bei dem Informationstechnikzentrum Bund (ITZBund) gespeichert seien. Nachdem die Petenten bei dem ITZBund entsprechende Anträge gestellt hatten, lehnte auch dieses die Anträge ab. Es agiere bezüglich der angeforderten Informationen lediglich als Dienstleister im Auftrag für das Ministerium und sei daher nicht verfügungsberechtigt. Verfügungsberechtigt sei vielmehr das Ministerium als Urheber der Information. Eine Übertragung der Verfügungsberechtigung sei nicht erfolgt.



80 Richtlinie 2003/4/EG des Europäischen Parlaments und des Rates vom 28. Januar 2003 über den Zugang der Öffentlichkeit zu Umweltinformationen und zur Aufhebung der Richtlinie 90/313/EWG des Rates (Umweltinformationsrichtlinie (RL 2003/4/EG))

Die Petenten wandten sich daraufhin an mich und rügten, dass auf diese Weise die E-Mail-Postfächer dem Informationszugang vollständig entzogen würden. Das Bundesministerium und das ITZBund hielten in den jeweiligen Verfahren an ihren Rechtsauffassungen fest.

Ich habe den Beteiligten mitgeteilt, dass ich bei isolierter Betrachtung die jeweiligen Bescheide nicht für offensichtlich rechtswidrig halte. Denn das Ministerium hatte aufgrund der Speicherung der E-Mail-Postfächer bei dem ITZBund keine unmittelbare technische Zugriffsmöglichkeit mehr auf diese. Die Argumentation des ITZBund, ihm fehle die Verfügungsberechtigung, halte ich für zutreffend. Verfügungsberechtigt ist in der Regel der Urheber der Information bzw. die sachnächste oder verfahrensführende Stelle. Dies ist nach meiner Einschätzung hier das Ministerium. Dies gilt auch dann, wenn der Inhaber des E-Mail-Postfachs mittlerweile aus der Behörde ausgeschieden ist. Denn allein dieser Stelle obliegt die Entscheidung, welche Informationen aus der auch zu privaten Zwecken gestatteten Nutzung des dienstlichen E-Mail-Postfachs der Privatsphäre ihres vormaligen Amtsträgers zuzuordnen sind und im Zuge eines Drittbeteiligungsverfahrens ggf. auszusondern wären.

Das Ergebnis, dass der Anspruch nach dem IFG durch die gewählte Konstruktion ins Leere geht, halte ich jedoch für nicht mit dem IFG vereinbar. Dies könnte allerdings nur über einen gegen das Ministerium gerichteten Wiederbeschaffungsanspruch oder über eine Verpflichtung des Ministeriums, dem ITZBund die Verfügungsberechtigung zu übertragen, aufgelöst werden. Die gewählte Konstruktion ist vergleichbar mit den Fällen, in denen sich eine Behörde einer privaten – und damit nicht informationspflichtigen – Stelle im Sinne des § 1 Abs. 1 S. 3 IFG bedient. Auch in diesen Fällen ist inzwischen anerkannt, dass der Grundsatz, dass die Behörde nicht zur (Wieder-)Beschaffung von Informationen verpflichtet ist, eine Modifikation erfahren muss.

Mangels Anordnungs- und Durchsetzungsbefugnissen und unter Berücksichtigung der Bestandskraft der genannten Bescheide hatte ich jedoch keine Handhabe, bei dem Ministerium die Herausgabe zu erwirken.

# 10 Bericht aus der ZASt



**Um eine wirkungs- und vertrauensvolle Zusammenarbeit der föderal organisierten deutschen Datenschutzaufsicht mit den europäischen Partnerbehörden, der Europäischen Kommission und dem Europäischen Datenschutzausschuss (EDSA) zu gewährleisten, beteiligt sich die Zentrale Anlaufstelle (ZASt) kontinuierlich konzeptionell und prozessorientiert an der Fortentwicklung der in diesem Zusammenhang berührten technisch-organisatorischen und rechtlichen Grundlagen.**

Die grenzüberschreitende Beschwerdebearbeitung ist nach der DSGVO grob in ein Vorverfahren zur Rollenklärung der europäischen Datenschutzaufsichtsbehörden (Art. 56 Abs. 1 DSGVO) sowie das Kooperationsverfahren mit Informationsaustausch, Amtshilfeersuchen, gemeinsamen Maßnahmen und insbesondere der Erarbeitung von Beschlussentwürfen (Art. 60 ff. DSGVO) gegliedert. Das Kooperationsverfahren mündet bei ausbleibendem Konsens unter den Datenschutzaufsichtsbehörden erforderlichenfalls in ein Verfahren zur Herstellung von Kohärenz durch den EDSA als übergeordnete Instanz (Art. 63 ff. DSGVO). Während 2022 gesamteuropäisch unter deutscher Beteiligung noch insgesamt 2.821 einzelne Verfahrensschritte im Rahmen der grenzüberschreitenden Fallbearbeitung (Vorverfahren, Kooperationsverfahren, Kohärenzverfahren) vollzogen wurden, davon 713 aus Deutschland ausgehend, sind die Zahlen für das Jahr 2025 kontinuierlich auf 4.631 einzelne Verfahrensschritte insgesamt mit deutscher Beteiligung und davon 1.517 aus Deutschland ausgehend gestiegen.

Das aktuelle Berichtsjahr der ZASt war zudem geprägt durch den europäischen Gesetzgebungsprozess zum Erlass einer Verfahrensverordnung sowohl auf nationaler als auch auf europäischer Ebene. Neben den fachlich zuständigen Mitarbeiterinnen und Mitarbeitern meines Hauses hat auch die ZASt das Verfahren konstruktiv bis zur am 12. Dezember 2025 erfolgten Veröffentlichung im Amtsblatt der Europäischen Union[81] unterstützt. Durch ein durchgehendes Fristenregime und neue Verfahrensschritte, die die Herstellung eines Konsenses unter den betroffenen Datenschutzaufsichtsbehörden fördern sollen, strebt die Verordnung eine stärkere Harmonisierung und Verfahrensbeschleunigung an, die zugleich zu einer weiteren Intensivierung der europäischen Zusammenarbeit der Datenschutzaufsichtsbehörden führen wird.

Die ZASt wird die deutschen Datenschutzaufsichtsbehörden darin unterstützen, die notwendigen Anpassungen von Prozessen und Arbeitsweisen der nationalen Zusammenarbeit bei grenzüberschreitenden Verfahren rechtzeitig bis zum Geltungsbeginn der Verfahrensverordnung zum 2. April 2027 vorzunehmen. Dies gilt insbesondere für notwendige Änderungen im DSGVO-Bereich des Binnenmarkt-Informationssystems der Europäischen Kommission (IMI), dem IT-Tool zur europäischen Verwaltungszusammenarbeit, das die Datenschutzaufsicht nutzt.

Zu diesem Zweck hat die ZASt bereits im aktuellen Berichtsjahr neue Bereiche der Zusammenarbeit, beispielsweise mit der nationalen IMI-Koordinatorin Deutschlands im Bundesverwaltungsamt, ausgelotet und etabliert. In diesem Zusammenhang fanden u. a. mehrere gegenseitige Besuche zur Vertiefung des fachlichen Austausches statt, und es wurde gemeinsam ein Leitfaden zur Nutzerverwaltung im IMI erstellt. Die ZASt hat darüber hinaus bestehende Formate gestärkt und ausgebaut, wie beispielsweise die nationalen IMI-Workshops. Sie hat sich für eine Übertragung dieses Formats der Zusammenarbeit auf die europäische Ebene erfolgreich eingesetzt. So ist für 2026 erstmalig ein Workshopformat der für IMI zuständigen Unterarbeitsgruppe des EDSA geplant.

81 Verordnung (EU) 2025/2518 des Europäischen Parlamentes und des Rates vom 26. November 2025 zur Festlegung zusätzlicher Verfahrensregelungen für die Durchsetzung der Verordnung (EU) 2016/679

Um die neue Rechtspflicht zur Durchsetzungsstatistik aus Art. 34 der Verfahrensverordnung erfüllen zu können und die Arbeit der Datenschutzaufsichtsbehörden auf dieser Grundlage quantifizierbarer zu machen, arbeitet die ZASt als Vorsitz des zuständigen Unterarbeitskreises der Datenschutzkonferenz (DSK) an einem nationalen Daten- und Definitionskranz mit. Mit diesem soll die statistische Darstellung der Arbeit der deutschen Datenschutzbehörden einheitlich auf europäischer Ebene eingebracht werden. Im Unterarbeitskreis erarbeitete Erläuterungen der europäischen Statistikanforderungen für die deutschen Datenschutzaufsichtsbehörden tragen dazu bei.

**Querverweis:**

5.2 Verfahrensverordnung für die Durchsetzung der DSGVO (VVO)

# 11 Über BfDI



## Key Facts – Personalentwicklung

Mitarbeiterzahl: 386
(+ 4,6 % Zuwachsrate im Vergleich zum Vorjahr)

50,7 % Frauen/49 % Männer/0,3 % divers

Durchschnittsalter der Beschäftigten:
43 Jahre

Durchschnittliche Behördenzugehörigkeit:
4,5 Jahre
(gerechnet ab Verselbständigung der Behörde 2016)

Budget 2025: 47 402 000 Euro

## 11.1 Personalentwicklung 2025

**Im Berichtsjahr hat meine Behörde weiterhin intensiv daran gearbeitet, offene Stellen zu besetzen und qualifizierte Fachkräfte zu gewinnen.**

Ein wichtiger Bestandteil der Personalgewinnung war die Teilnahme an Karrieremessen, um meine Behörde als attraktive Arbeitgeberin zu präsentieren und direkt mit interessierten Fachkräften in Kontakt zu treten. So war meine Behörde auf den Fakultätskarrieretagen in Bonn und Köln, dem Unternehmenstag der Hochschule Bonn-Rhein-Sieg und dem Fachbereichstag der Hochschule des Bundes vertreten, wo potenzielle Bewerberinnen und Bewerber aus verschiedenen Fachrichtungen gezielt angesprochen werden konnten.

Zum Stichtag 31. Dezember 2025 verfügte meine Behörde insgesamt über 386 Mitarbeiterinnen und Mitarbeiter. Auch wenn mein Haus im Jahr 2025 durch insgesamt 32 neue Kolleginnen und Kollegen verstärkt wurde, musste ich 15 Personalabgänge verzeichnen. Somit konnte mein Haus im Vergleich zum Vorjahr um 17 Personen anwachsen. Vorhandene Einstellungspotenziale werden weiter aktiv genutzt. Mein Ziel ist, diese durch weitere Einstellungen noch im ersten Halbjahr 2026 auszuschöpfen.

Mein Haus bietet vielfältige Tätigkeitsfelder, die regelmäßig auch internationale Bezüge haben. Daher haben im Jahr 2025 sechs meiner Mitarbeiterinnen und Mitarbeiter an dem Programm zum Personalaustausch zwischen den Datenschutzaufsichtsbehörden des EWR einschließlich des EDSB und des EDSA teilgenommen. Im Rahmen des Austauschprogramms hat mein Haus einen Kollegen der französischen Aufsichtsbehörde „CNIL“ für drei Monate aufgenommen.

## 11.2 Zahlen und Fakten zum Berichtsjahr

**Die Arbeit meiner Behörde besteht nicht nur aus den hier umfangreich berichteten Fällen, sondern ist auch stark von einer Vielzahl kleinerer Verwaltungsverfahren geprägt. Die Statistik zeigt: Das Arbeitsaufkommen meiner Behörde ist in den vergangenen Jahren stark gestiegen ist.**

### Beschwerden und Anfragen

Im Berichtsjahr wurden insgesamt 11 824 Beschwerden und Anfragen an mich gerichtet. Dies entspricht fast dem Allzeithoch aus dem Jahr 2018, als mich im Rahmen der DSGVO-Einführung 11 912 Beschwerden und Eingaben erreichten. Der Anstieg der Fallzahlen spiegelt sich in allen Referaten meines Hauses wider.

| Beschwerden und Anfragen | 2022 | 2023 | 2024 | 2025 |
|---|---|---|---|---|
| Allgemeine Anfrage | 4434 | 5162 | 5225 | 6330 |
| Beschwerde Art. 77 DSGVO | 2115 | 2513 | 3313 | 5329 |
| Beschwerde Art. 80 DSGVO | 3 | 11 | 10 | 11 |
| Beschwerde § 60 BDSG | 29 | 50 | 75 | 84 |
| Eingabe gegen Nachrichtendienste | 38 | 46 | 47 | 70 |

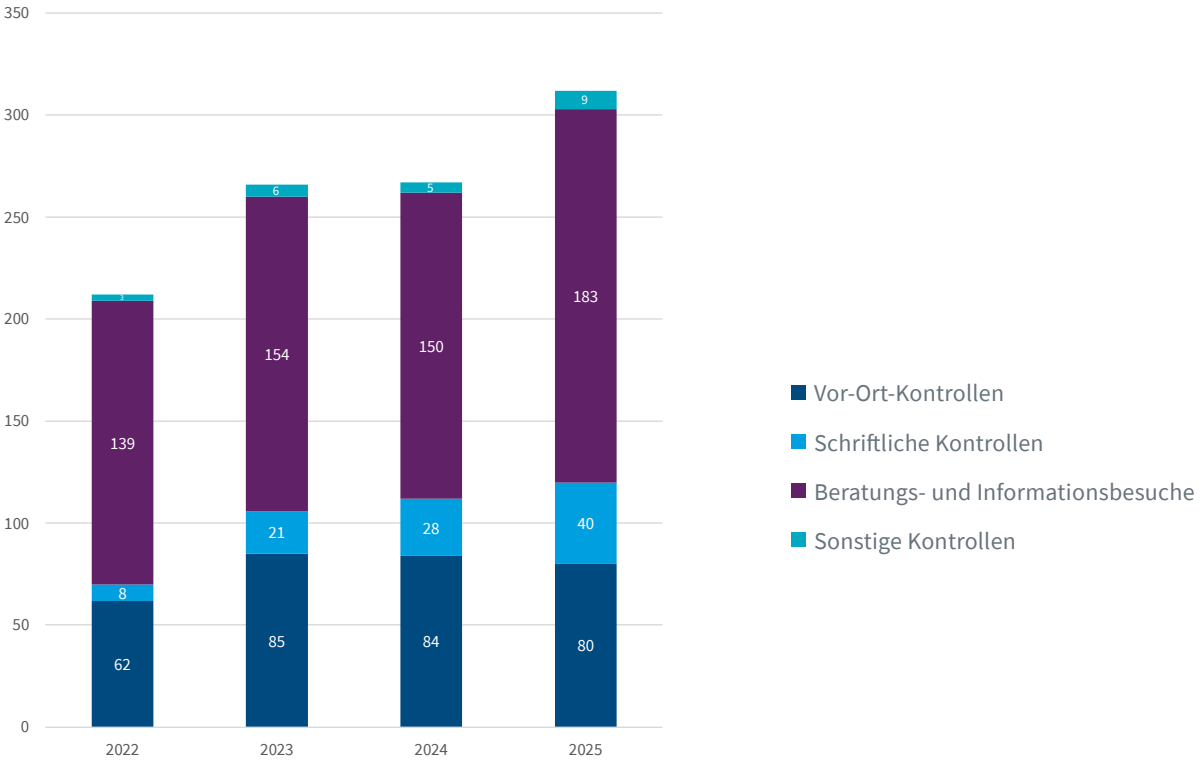
Sowohl bei den allgemeinen Anfragen als auch bei den Beschwerden nach DSGVO und BDSG (siehe Tabelle) kann ein klarer Anstieg des Volumens verzeichnet werden. Dabei hat sich die Zahl der förmlichen Beschwerden nach Art. 77 DSGVO besonders dynamisch entwickelt und innerhalb von zwei Jahren mehr als verdoppelt. Neben schriftlichen bzw. elektronischen Anfragen sowie Beschwerden haben meine Mitarbeiterinnen und Mitarbeiter in 3091 Fällen Personen telefonisch beraten.

**Beratung und Kontrolle**

Als Aufsichtsbehörde stellen Beratung und Kontrolle wichtige Arbeitsbereiche für meine Behörde dar, die mitunter stark vom persönlichen Kontakt mit den beaufsichtigten verantwortlichen Stellen leben. Im Berichtsjahr konnte ich insbesondere die Beratungs- und Informationsbesuche steigern. Bei diesen Terminen werden konkrete Problemstellungen und datenschutzfreundliche Lösungsmöglichkeiten besprochen. Oftmals werden die Themen von den beaufsichtigten Stellen an mich herangetragen.

Die Anzahl der Kontrolltermine bewegt sich im Berichtsjahr auf dem Niveau des Vorjahres.

**Beratungen und Kontrollen seit 2022**



### Abhilfemaßnahmen

Meine Kontrolltätigkeit mündete in einer hohen Anzahl an Maßnahmen. Im Berichtsjahr hat meine Behörde 129 aufsichtsrechtliche Maßnahmen vorgenommen, wie z. B. Verwarnungen, Anweisungen oder die Festsetzung von Zwangsgeldern.

**Eine ausführliche Auflistung der Maßnahmen findet sich auf meiner Webseite**

(QR-Code klicken oder scannen)

### Meldungen von Datenschutzverstößen

Vergleichsweise stabil blieb die Anzahl der Meldungen von Datenschutzverstößen. Im Berichtsjahr habe ich 9170 Meldungen entgegengenommen.

### Förmliche Begleitung von Rechtsetzungsvorhaben

Gemäß § 21 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) haben die federführenden Ressorts mich bei der Erstellung von Gesetzesvorlagen frühzeitig zu beteiligen, soweit diese meine Aufgaben berühren. Aus der Statistik für das Berichtsjahr lässt sich eine insgesamt geringere Anzahl an Beteiligungen erkennen. Die geringere Anzahl ist im Wesentlichen auf die Bundestagswahl zurückzuführen. Mein Ziel ist, mit einer lösungsorientierten Beratung bereits vor der formellen Beteiligung von den federführenden Ressorts vertrauensvoll in die Erarbeitung von Gesetzesentwürfen einbezogen zu werden.

In die Gesetzgebung selbst wurde ich auch durch den Deutschen Bundestag eingebunden. In zwei Fällen wurde ich von Ausschüssen als Sachverständige gehört. Auf nationaler Ebene wurde ich darüber hinaus in 28 Fällen zur Prüfung von Dateianordnungen bei Sicherheitsbehörden beteiligt.

Auf europäischer Ebene war ich außerdem bei der Erstellung von 12 Verordnungen und einer Richtlinie eingebunden.

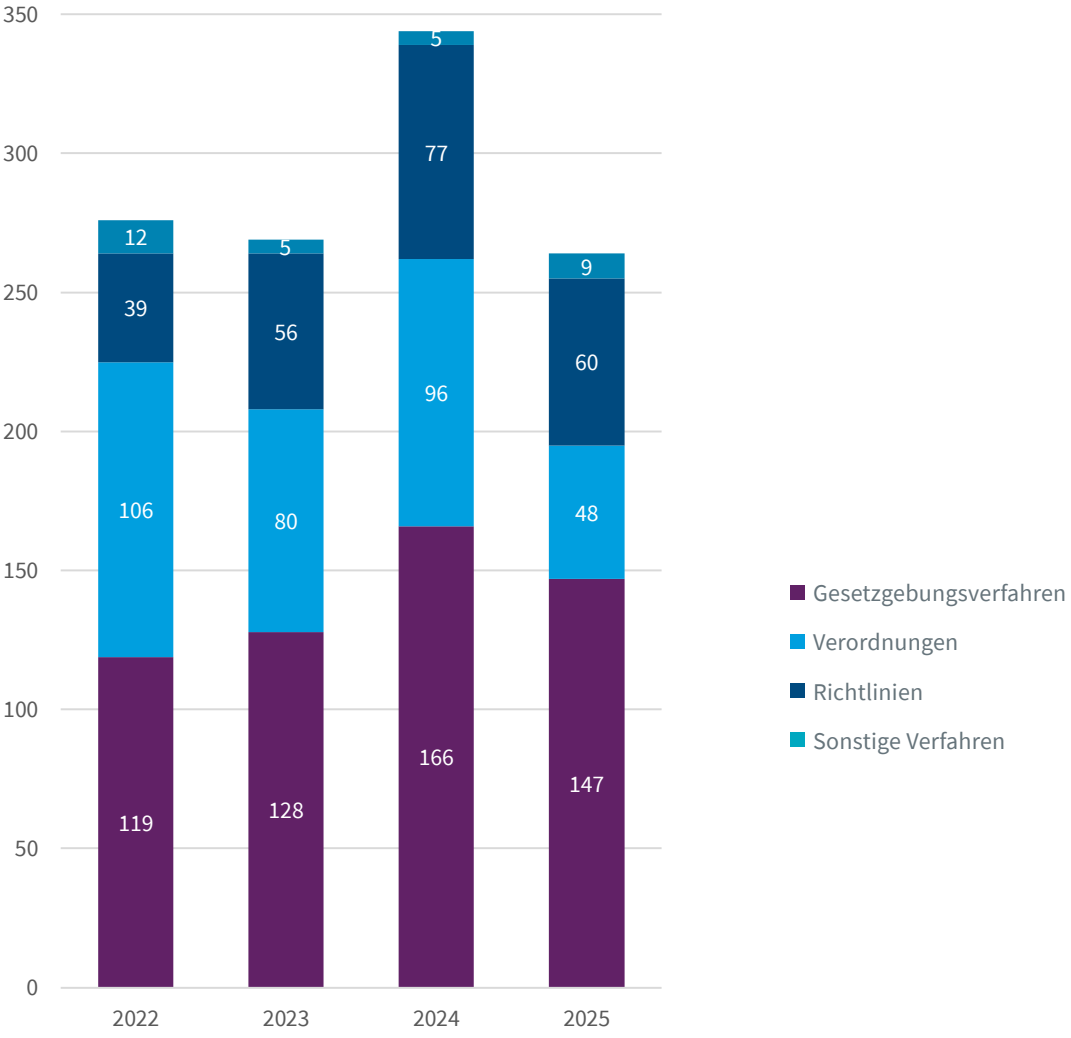
| Meldungen von Datenschutzverstößen | 2022 | 2023 | 2024 | 2025 |
|---|---|---|---|---|
| Meldungen nach Art. 33 DSGVO | 10 614 | 9 234 | 8 740 | 9 110 |
| Meldungen nach § 169 TKG | 44 | 29 | 47 | 60 |

### Gremiensitzungen

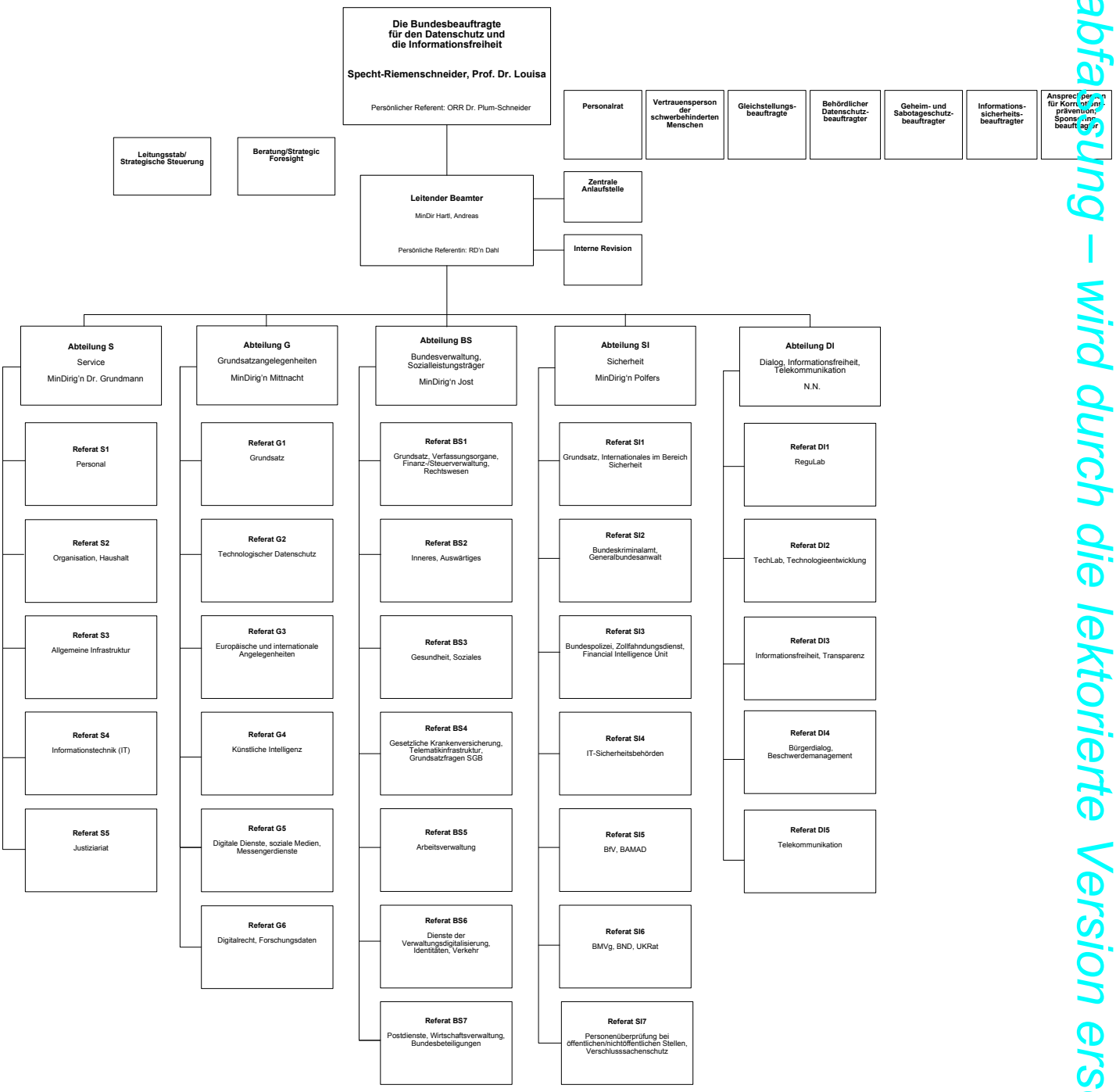
Über meine Mitgliedschaft in Organisationen wie der Datenschutzkonferenz (DSK), dem Europäischen Datenschutzausschuss (EDSA) und vielen weiteren – oft internationalen – Gremien[82] bin ich im Austausch mit unterschiedlichsten Akteuren im Bereich des Datenschutzes.

Im Berichtsjahr haben meine Mitarbeitenden als (Co-) Vorsitz/Rapporteur insgesamt 313 Sitzungen geleitet und darüber hinaus als Mitglied an 852 Sitzungen teilgenommen. In diese Gremien hat mein Haus vier Entschließungs- bzw. Beschlussentwürfe eingebracht.

82 Liste der Gremien unter: www.bfdi.bund.de/tb-34-gremien



BfDI
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit




**Anschrift:**
Dienstsitz Bonn: Graurheindorfer Str. 153, 53117 Bonn
Postfach 14 68, 53004 Bonn

Verbindungsbüro
Berlin: Spittelmarkt 11, 10117 Berlin

**Erreichbarkeit:**
Telefon: 0228/997799-0
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

Stand: 14. April 2026

## Abkürzungsverzeichnis

| | |
|---|---|
| a. a. O. | am angegebenen Ort |
| AA | Auswärtiges Amt |
| Abs. | Absatz |
| AKIF | Arbeitskreis Informationsfreiheit |
| Art. | Artikel |
| Az. | Aktenzeichen |
| BA | Bundesagentur für Arbeit |
| BAMAD | Bundesamt für den Militärischen Abschirmdienst |
| bDSB | behördliche Datenschutzbeauftragte |
| BDSG | Bundesdatenschutzgesetz |
| Berlin Group | International Working Group on Data Protection in Technology |
| BfDI | Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit |
| BfJ | Bundesamt für Justiz |
| BfArM | Bundesinstitut für Arzneimittel und Medizinprodukte |
| BfV | Bundesamt für Verfassungsschutz |
| BKA | Bundeskriminalamt |
| BKAG | Bundeskriminalamtgesetz |
| BMDS | Bundesministerium für Digitales und Staatsmodernisierung |
| BMF | Bundesministerium der Finanzen |
| BMG | Bundesministerium für Gesundheit |
| BMI | Bundesministerium des Innern und für Heimat |
| BMVg | Bundesministerium der Verteidigung |
| BND | Bundesnachrichtendienst |
| BNDG | Gesetz über den Bundesnachrichtendienst |
| BPA | Bundespresseamt |
| BPOL | Bundespolizei |
| BPolG | Bundespolizeigesetz |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BSIG | Gesetz über das Bundesamt für Sicherheit in der Informationstechnik |
| BT-Drs. | Bundestagsdrucksache |
| BTPOL | Polizei des Deutschen Bundestages |
| Buchst. | Buchstabe |
| BVA | Bundesverwaltungsamt |
| BVerfG | Bundesverfassungsgericht |
| BVerfSchG | Bundesverfassungsschutzgesetz |
| BwSchutzG | Bundeswehr-Schutz-Gesetz |
| BZR | Bundeszentralregister |
| BZRG | Bundeszentralregistergesetz |
| bzw. | beziehungsweise |
| bspw. | beispielsweise |
| CCC | Chaos Computer Club |
| CIC ESG | „Cross-Regulatory Interplay and Cooperation“ Expert Subgroup |
| CNIL | Commission Nationale de l’Informatique et des Libertés (Französische Datenschutzaufsichtsbehörde) |
| COVID-19 | Coronavirus |
| CSAM | Child sexual abuse material |
| CSA-VO | Verordnung zum Auffinden von Material des sexuellen Online-Kindesmissbrauchs |
| CSC | Coordinated Supervision Committee |

| | |
|---|---|
| DMA | Digital Markets Act |
| DNA | Desoxyribonukleinsäure |
| DPA | Data Processing Addendum |
| DPF | EU-U.S. Data Privacy Framework |
| DSA | Digital Services Act |
| DSC | Datenschutzcockpit |
| DSGVO | Datenschutz-Grundverordnung |
| DSK | Konferenz der unabhänigegen Datenschutzbehörden des Bundes und der Länder |
| DUA Act | Data Use and Access Act |
| ePrivacy-Richtlinie | Datenschutzrichtlinie für elektronische Kommunikation |
| ECRIS | European Criminal Records Information System |
| ECRIS-RI | ECRIS Reference Implementation |
| EDHS | European Health Data Space Verordnung |
| EDSB | Europäischer Datenschutzbeauftragter |
| EDSA | Europäischer Datenschutzausschuss |
| eEB | elektronische Ersatzbescheinigung |
| eFBS | einheitliches Fallbearbeitungssystem |
| eGK | elektronische Gesundheitskarte |
| EHDS | European Health Data Space |
| EHDS-VO | Verordnung über den Europäischen Gesundheitsraum |
| eID | elektronische Identität |
| eIDAS VO | Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt |
| EnSiG | Energiesicherungsgesetz |
| ENTRI | European Network for Transparency and Right to Information |
| ePA | elektronische Patientenakte |
| EPO | Europäische Patentorganisation |
| eSIM | elektronische SIM-Karte |
| EU | Europäische Union |
| EUDI-Wallet | Europäische Brieftaschen für die Digitale Identität |
| EuGH | Europäischer Gerichtshof |
| EWR | Europäischer Wirtschaftsraum |
| EZB | Europäische Zentralbank |
| FDZ | Forschungsdatenzentrum Gesundheit |
| ff. | fortfolgende |
| FIU | Financial Intelligence Unit |
| FKS | Finanzkontrolle Schwarzarbeit |
| gematik | Gesellschaft für Telematik |
| ggf. | gegebenenfalls |
| grds. | grundsätzlich |
| GZD | Generalzolldirektion |
| HZÄ | Hauptzollämter |
| ICIC | Internationale Konferenz der Informationsfreiheitsbeauftragten |
| IDNr | Identifikationsnummern |
| IDNrG | Identifikationsnummerngesetz |
| i. d. R. | in der Regel |
| IFG | Informationsfreiheitsgesetz |
| IFK | Konferenz der Informationsfreiheitsbeauftragten |
| IfSG | Infektionsschutzgesetz |
| IMI | Binnenmarkt-Informationssystem |
| INPOL | Polizeiliche Informationssystem |

| | |
|---|---|
| INPOL-Z | Zentrale Datenbank des BKA |
| IT | Informationstechnologie |
| ITZBund | Informationstechnikzentrum Bund |
| i. V. m. | in Verbindung mit |
| JI-Richtlinie | Richtlinie zum Datenschutz bei Polizei und Justiz |
| KMU | Kleine und Mittlere Unternehmen |
| KI | Künstliche Intelligenz |
| KI-VO | KI-Verordnung |
| MAD | Militärischer Abschirmdienst |
| MADG | Gesetz über den Militärischen Abschirmdienst |
| META | Meta Platforms Ireland Ltd. |
| MRG-E | Medizinregistergesetz |
| MS | Mitgliedsstaaten |
| NADIS | Nachrichtendienstliches Informationssystem |
| NGO | Nichtregierungsorganisation |
| NIS-2-Richtlinie | Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union |
| NIS-2-Umsetzungsgesetz | Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagments in der Bundesverwaltung |
| NOOTS | Nationales Once-Only-Technical-System |
| Nr. | Nummer |
| o. g. | oben genannt |
| OIDA | Operative Informations- und Datenanalysesystem |
| Omnibus | Ein Omnibusgesetzgebungsverfahren zielt darauf ab, mit einem einzigen Gesetzesvorhaben gleichzeitig mehrere bereits bestehende Rechtsakte zu ändern |
| OSINT | Open Source Intellligence |
| OVG | Oberverwaltungsgericht |
| OWiG | Gesetz über Ordnungswidrigkeiten |
| P 20 | Polizei 20/20 |
| PAuswG | Gesetz über Personalausweise und den elektronischen Identitätsnachweis |
| S. | Satz |
| SchwarzArbG | Modernisierung des Schwarzarbeitsbekämpfungsgesetzes |
| SchwarzArbMoDiG | Gesetz zur Modernisierung und Digitalisierung der Schwarzarbeitsbekämpfung |
| SGB | Sozialgesetzbuch |
| SGB V | Sozialgesetzbuch Fünftes Buch |
| SI | Abteilung Sicherheit |
| SMC | „Mid-Cap“-Unternehmen |
| sog. | sogenannte |
| Steuer-ID | Steuer-Identifikationsnummer |
| StPO | Strafprozessordnung |
| SÜG | Sicherheitsüberprüfungsgesetz |
| TB | Tätigkeitsbericht |
| TDDDG | Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz |
| THW | Technische Hilfswerk |
| TK | Techniker Krankenkasse |
| Trilog | EU-Kommission, Rat der EU und Europäisches Parlament |
| u. a. | unter anderem |
| UN | United Nations |
| UIG | Umweltinformationsgesetz |

| | |
|---|---|
| US/U.S. | United States |
| USA | Vereinigte Staaten von Amerika |
| usw. | und so weiter |
| v. a. | vor allem |
| VG | Verwaltungsgericht |
| Vgl. | vergleiche |
| VIS | Visa-Informationssystem |
| VK | Vereinigtes Königreich |
| VO | Verordnung |
| VS | Vermittlungsstelle |
| VVO | Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO |
| z. B. | zum Beispiel |
| ZASt | Zentrale Anlaufstelle |
| ZfS | Zentralstelle für Sanktionsdurchsetzung |
| ZFdG | Zollfahndungsdienstgesetz |
| ZITiS | Zentrale Stelle für Informationstechnik im Sicherheitsbereich |
| ZKA | Zollkriminalamt |
| ZollVG | Zollverwaltungsgesetz |
| 6G | Sechste Generation Mobilfunk |