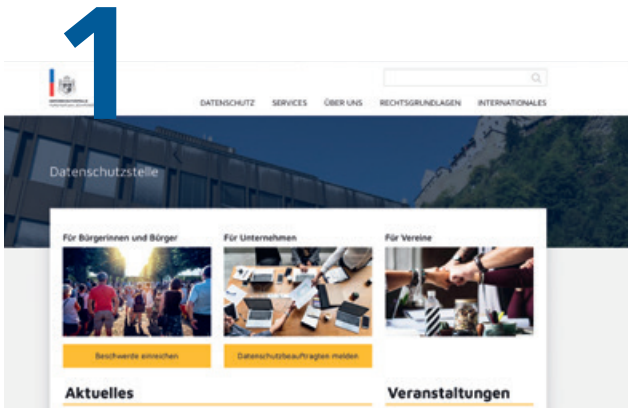
2025

TÄTIGKEITSBERICHT

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Inhaltsverzeichnis



Impressum

Herausgeber: Datenschutzstelle Fürstentum Liechtenstein
Grafische Gestaltung und Druck: Gutenberg AG, Schaan
Text: Datenschutzstelle Fürstentum Liechtenstein
Bilder: Stockphoto.com, Pixabay.com, Pexels.com, 123rf.com, Datenschutzstelle Fürstentum Liechtenstein

Vorwort

Sie haben es vermutlich schon bemerkt: Unser Tätigkeitsbericht präsentiert sich in diesem Jahr in einem teilweise neuen Design. Diese Veränderung beruht auf zwei Gründen. Erstens markiert das neue Erscheinungsbild den Beginn meiner zweiten Amtszeit, die am 1. Januar 2026 begonnen hat. Vor acht Jahren übernahm ich die Leitung der Datenschutzstelle (DSS) nahezu zeitgleich mit dem Wirksamwerden der Datenschutz-Grundverordnung (DSGVO). Für das erneute Vertrauen der Regierung und des Landtages danke ich ausdrücklich. Die behutsame Modernisierung des Berichts soll diesen Übergang sichtbar machen und einen neuen Abschnitt meiner Amtsführung unterstreichen.

Zweitens trägt das neue Design der inhaltlichen Dynamik des Datenschutzes Rechnung. Datenschutz ist keine statische Rechtsmaterie, sondern entwickelt sich kontinuierlich weiter – insbesondere im Spannungsfeld technologischer Innovationen, zunehmender Digitalisierung und datengetriebener Geschäftsmodelle. Das aktualisierte Erscheinungsbild verdeutlicht symbolisch, dass sich rechtliche Rahmenbedingungen wie technische Realitäten stetig verändern und der Datenschutz diesen Entwicklungen aktiv begegnen muss.

Das Jahr 2025 hat diese Dynamik besonders bestätigt. Die fortschreitende Integration künstlicher Intelligenz (KI) in Verwaltung, Wirtschaft und Bildung warf neue Fragen zur Rechtmässigkeit der Datenverarbeitung, zu automatisierten Entscheidungen sowie zur Transparenz von Trainingsdaten auf. Die KI-Verordnung ist in Liechtenstein mangels Übernahme ins EWR-Recht zwar noch nicht verbindlich, entfaltet jedoch faktische Vorwirkung. Verantwortliche Stellen sollten ihre Systeme frühzeitig an künftigen Anforderungen ausrichten.

Auch auf europäischer Ebene war 2025 von Weiterentwicklungen geprägt. Eine neue EU-Verordnung harmonisiert zusätzliche Verfahrensregeln zur Durchsetzung der DSGVO in grenzüberschreitenden Verfahren. Mit dem Digital-Omnibus-Paket sollen Digitalrechtsakte punktuell angepasst und besser aufeinander abgestimmt werden. Diese Reformen stehen für die fortschreitende Konsolidierung des europäischen Digitalrechtsrahmens. Konkrete langfristige Auswirkungen auf Aufsichtspraxis und Pflichten der Verantwortlichen, insbesondere kleiner und mittlerer Unternehmen, lassen sich noch nicht abschliessend beurteilen. Klar ist jedoch: Die rechtlichen Rahmenbedingungen bleiben in Bewegung.

Dr. Marie-Louise Gächter, Leiterin Datenschutzstelle

Das Berichtsjahr war zudem von zunehmender Komplexität in sämtlichen Tätigkeitsbereichen der DSS geprägt. Neben einer quantitativen Zunahme von Anfragen, Beschwerden und Meldungen über Datenschutzverletzungen stiegen auch die qualitativen Anforderungen. Eine kritischere Haltung betroffener Personen traf auf wachsende Erwartungen an Digitalisierung und KI. Die DSS war daher wiederholt gefordert, eine vermittelnde Rolle einzunehmen. Neue europäische Digitalrechtsakte verursachten zusätzlichen Analyse- und Abstimmungsaufwand.

Der Bericht dokumentiert diese Entwicklungen, benennt Defizite, würdigt Fortschritte und gibt Orientierung für die Praxis. Datenschutz bleibt eine Querschnittsaufgabe, die rechtliche Präzision, technische Expertise und gesellschaftliche Verantwortung erfordert. Dass wir unseren Auftrag unter anspruchsvollen Bedingungen erfüllen konnten, ist dem Engagement und der Fachkompetenz aller Mitarbeitenden der DSS zu verdanken. In diesem Spannungsfeld wird die DSS auch künftig unabhängig und grundrechtsorientiert handeln.

Vaduz, im April 2026

«Für die Vermittlung von Fachinformationen nutzt die DSS vor allem vier Kanäle: Veranstaltungen und Vorträge, Newsletter, ihre Internetseite und individuelle Beratungen.»

1. Öffentlichkeitsarbeit

Der gesetzliche Auftrag zur Wissensvermittlung im Datenschutz unterstreicht die zentrale Bedeutung einer aktiven, transparenten und adressatengerechten Öffentlichkeitsarbeit für die Tätigkeit der DSS. Datenschutzrechtliche Grundsätze, aktuelle regulatorische Entwicklungen sowie die Positionen nationaler und europäischer Aufsichtsbehörden und Gerichte müssen verständlich aufbereitet und einer breiten Öffentlichkeit zugänglich gemacht werden.

Die Öffentlichkeitsarbeit dient aber auch dazu, der Verbreitung von nicht-datenschutzkonformen Praktiken auf einer breiten Ebene entgegenzuwirken, um den Verantwortlichen die Möglichkeit zu bieten, ihre Datenverarbeitungen in Übereinstimmung mit den gesetzlichen Vorgaben zu bringen.

Darüber hinaus informierte die DSS unter anderem auch über aktuelle datenschutzrechtliche Fragestellungen im digitalen Umfeld, die vor allem Bürgerinnen und Bürger betreffen – wie etwa die Datenübermittlungen von TikTok in den Drittstaat China und deren kritischer Bewertung nach der DSGVO oder das KI-Training durch LinkedIn und die Empfehlung zur Wahrnehmung des Widerspruchsrechts. Ziel ist es, betroffenen Personen eine fundierte Orientierung zu ermöglichen und das Bewusstsein für datenschutzrechtliche Risiken nachhaltig zu stärken.

In Bezug auf die Verantwortlichen bildete wie bereits im Vorjahr auch 2025 insbesondere das Thema KI einen zentralen Schwerpunkt der Wissensvermittlung. In kaum einem anderen Bereich ist der Informations- und Orientierungsbedarf derzeit so ausgeprägt. Vor dem Hintergrund der dynamischen technischen Entwicklung und der zunehmenden praktischen Implementierung von KI-Systemen war es der DSS ein besonderes Anliegen, die Anforderungen der KI-Verordnung frühzeitig zu vermitteln – ungeachtet ihrer noch ausstehenden formalen Übernahme in das liechtensteinische Recht.

Die Informationsarbeit konzentrierte sich dabei insbesondere auf die Regelungen zu verbotenen KI-Praktiken, auf die Verpflichtung zur Sicherstellung angemessener KI-Kompetenz (AI Literacy) sowie auf Transparenzanforderungen gegenüber Nutzerinnen und Nutzern, aber auch im Verhältnis zwischen Anbieter und Betreiber. Diese Vorgaben gelten innerhalb der Europäischen Union (EU) bereits unmittelbar und entfalten aus Sicht der DSS auch für Verantwortliche in Liechtenstein eine faktische Relevanz, die im Rahmen einer vorausschauenden und verantwortungsvollen Compliance nicht unberücksichtigt bleiben darf.

Diese Erkenntnisse zeigen erneut deutlich auf, dass Datenschutz ohne eine aktive und frühzeitige Informations- bzw. Wissensvermittlung seitens der Aufsichtsbehörden nicht die Rolle bei den öffentlichen und privaten Stellen spielen kann, die ihm der Gesetzgeber zugedacht hat. Die Wissensvermittlung darf sich ausserdem nicht damit begnügen, auf Neuerungen hinzuweisen, sondern muss nach wie vor auch den Bedarf an Grundwissen abdecken.

Für die Vermittlung von Fachinformationen nutzt die DSS vor allem vier Kanäle: Veranstaltungen und Vorträge, Newsletter, Internetseite und individuelle Beratungen. Insbesondere das Zusammenwirken dieser Kommunikationskanäle ermöglicht es, eine sehr grosse Zahl an Adressatinnen und Adressaten zu erreichen.

1.1 Veranstaltungen

Der **19. Datenschutztag** fand wie üblich zu Beginn des Jahres am 28. Januar im Gemeindesaal in Triesen statt und widmete sich den datenschutzrechtlichen Herausforderungen vernetzter Fahrzeuge. Unter dem Titel «Mit Vollgas in die Zukunft – Was weiss mein Auto über mich?» stand die zunehmende Digitalisierung der Automobilindustrie im Mittelpunkt. Moderne Fahrzeuge sind heute mit einer Vielzahl von Sensoren, Assistenzsystemen und Online-Diensten ausgestattet. Dabei werden umfangreiche personenbezogene Daten erhoben, etwa zum Fahrverhalten, zu Standortbewegungen, zur Nutzung von Infotainment-Systemen oder zur Interaktion mit mobilen Endgeräten.

Im Rahmen der Veranstaltung beleuchtete der Hauptreferent, Markus Reuter von netzpolitik.org, auf Grundlage aktueller journalistischer Recherchen, welche Daten moderne Fahrzeuge erfassen und welche Risiken sich daraus für die Privatsphäre ergeben können. Im Anschluss diskutierten er, die Leiterin der DSS, sowie Franziska Füglistaler von cardossier über technische Entwicklungen, rechtliche Rahmenbedingungen und ethische Fragestellungen rund um Fahrzeugdaten.

Die Veranstaltung, die auf sehr grosses Interesse stiess, bot den rund 120 Teilnehmenden eine praxisnahe Einordnung eines Themenfeldes, das angesichts zunehmender Vernetzung und datengetriebener Geschäftsmodelle weiter an Bedeutung gewinnen wird.

Am 10. November führte die DSS ihr jährliches **Vernetzungstreffen für Datenschutzbeauftragte** durch. Ziel der Veranstaltung war es, aktuelle Entwicklungen im Datenschutzrecht praxisnah zu beleuchten, Erfahrungen auszutauschen und den Dialog mit Datenschutzbeauftragten sowie Verantwortlichen weiter zu stärken. Ein Schwerpunkt lag auf der Auswertung der Beratungs-, Beschwerde- und Meldetätigkeit im Berichtsjahr. Besonders häufig betrafen Beschwerden das Auskunftsrecht nach Art. 15 DSGVO, Fragen der Rechtsgrundlage nach Art. 6 DSGVO sowie Informations- und Löschpflichten. Wiederkehrende Problemfelder zeigten sich insbesondere bei unzureichend konkreten Auskünften, fehlender vorgängiger Festlegung der Rechtsgrundlage sowie uneinheitlichen internen Prozessen. Auch gemeldete Datenschutzverletzungen – etwa durch Phishing, Fehlversand von E-Mails oder Cyberangriffe – verdeutlichten die anhaltende Relevanz technischer und organisatorischer Schutzmassnahmen.

Ein weiterer Programmpunkt des Vernetzungstreffens widmete sich aktuellen Entwicklungen im In- und Ausland. Behandelt wurden unter anderem neue Entscheidungen des Europäischen Gerichtshofs (EuGH) zu Fragen wie etwa den Rechtsgrundlagen für Datenverarbeitungen oder der Pseudonymisierung und Anonymisierung sowie die geplante Verfahrensharmonisierung auf EU-Ebene. Ergänzend erfolgte eine Einordnung zentraler Digitalrechtsakte wie KI-Verordnung, Digital Services Act (DSA) und Digital Markets Act (DMA).

Zudem stellte die DSS die nationalen Ergebnisse der auf EU/EWR-Ebene koordinierten Aktion 2025 zum Recht auf Löschung nach Art. 17 DSGVO vor («Coordinated Enforcement Framework»). Die Befragung von fünf liechtensteinischen Organisationen zeigte, dass zwar grundsätzlich Verfahren und Prozesse zur Umsetzung dieses Betroffenenrechts in den Institutionen bestehen, jedoch teils grosse Unterschiede in Struktur, Dokumentation, Transparenz und technischer Ausgestaltung vorhanden sind. Daraus leitete die DSS konkrete Empfehlungen für Verantwortliche und insbesondere für ein umfassendes und nachvollziehbares Löschkonzept ab.

Das Vernetzungstreffen bot damit erneut einen vertieften Überblick über Vollzugspraxis, rechtliche Entwicklungen und nach wie vor bestehende Problemfelder und leistete einen wichtigen Beitrag zur Stärkung der datenschutzrechtlichen Compliance in Liechtenstein.

Am 6. Mai veranstaltete die DSS bereits zum dritten Mal einen **Kinoabend** mit anschliessender Podiumsdiskussion im Skino. Die Veranstaltung im Rahmen der Reihe «Datenschutz goes Cinema» stand unter dem Titel «Identitätsdiebstahl: Du hast vielleicht nichts zu verbergen, aber etwas zu verlieren – deine Identität» und war innerhalb weniger Tage ausgebucht – ein deutliches Zeichen für das grosse öffentliche Interesse am Thema.

Gezeigt wurde der Thriller *Das Netz* von Irwin Winkler (USA 1995), in dem eine von Sandra Bullock gespielte Computerexpertin Opfer eines perfiden Identitätsdiebstahls wird. Der Film verdeutlichte eindrücklich, wie existenziell digitale Identität für die gesellschaftliche und wirtschaftliche Teilhabe ist – und wie gravierend die Folgen ihres Missbrauchs sein können. Trotz seines Erscheinungsjahres 1995 sind die dargestellten Risiken angesichts zunehmender Digitalisierung, Social Media und datengetriebener Geschäftsmodelle aktueller denn je.

Im Anschluss diskutierten Tina Groll, Journalistin und Expertin für Identitätsdiebstahl und Internetkriminalität, Vertreter der Landespolizei sowie die Leiterin der DSS über typische Erscheinungsformen von Identitätsmissbrauch, Präventionsmöglichkeiten und rechtliche Konsequenzen. Besonderes Gewicht erhielt der praxisnahe Austausch: Welche ersten Schritte sind im Schadensfall zu setzen? Welche Beweise sollten gesichert werden? Welche Rolle spielen strafrechtliche Anzeigen und zivilrechtliche Ansprüche?

Zudem wurde der datenschutzrechtliche Kontext beleuchtet. Identitätsdiebstahl ist regelmässig mit unrechtmässiger Datenverarbeitung verbunden; entsprechend können Betroffenenrechte – insbesondere auf Auskunft, Berichtigung und Löschung – ein wichtiges Instrument zur Schadensbegrenzung darstellen. Die Veranstaltung klang mit einem Apéro aus und bot Raum für vertiefende Gespräche zwischen Referierenden und Publikum.

Mit dem neuen Veranstaltungsformat **«KI-Frühstück»** beschritten die DSS und die Hochschule Luzern im Jahr 2025 bewusst neue Wege der Wissensvermittlung. Ziel war es, aktuelle Fragen rund um den Einsatz von KI in kompakter Form, praxisnah und im direkten Dialog zu diskutieren – und dies in ungezwungener Atmosphäre bei Kaffee und frischen Gipfeli.

Die Resonanz übertraf sämtliche Erwartungen: Der erste Termin am 23. Juni im Haus Gutenberg in Balzers war innerhalb von 30 Minuten ausgebucht. Aufgrund der grossen Nachfrage wurde kurzfristig ein zweiter Termin am 17. September mit erweiterter Teilnehmerzahl angesetzt. Dieses hohe Interesse verdeutlichte den erheblichen Informationsbedarf im Bereich KI und Compliance.

In drei Kurzreferaten wurden zentrale Fragestellungen beleuchtet: Die Leiterin der DSS thematisierte die Pflicht zur Sicherstellung von KI-Kompetenz gemäss Art. 4 der KI-Verordnung und deren Bedeutung für private wie öffentliche Stellen. Ein Wirtschaftsinformatiker und KI-Praktiker zeigte praxisnah Anwendungsfälle, Chancen und Risiken des KI-Einsatzes in Unternehmen auf, einschliesslich unvorhergesehener Effekte im operativen Alltag. Ein Spezialist für Cybersicherheit widmete sich schliesslich der Frage, inwieweit Datenschutz und Datensicherheit in KI-Modellen technisch realisierbar sind – und wo die Grenzen liegen.

Beim zweiten Termin wurde das Programm um einen zusätzlichen Vortrag zu den Transparenzpflichten nach der KI-Verordnung ergänzt. Dabei ging es insbesondere um Informationspflichten, Kennzeichnungserfordernisse und die Anforderungen an nachvollziehbare Kommunikation beim Einsatz von KI-Systemen.

Die anschliessende angeregte Diskussion zeigte, dass das gewählte Format – konzentrierte Inputs, gefolgt von einer offenen Fragerunde – den Nerv der Zeit trifft. Fachlicher Tiefgang und niederschwelliger Austausch schlossen sich dabei keineswegs aus; im Gegenteil: Zwischen Kaffeetasse und Gipfeli wurden hochkomplexe Fragen mit bemerkenswerter Präzision diskutiert.

Aufgrund der positiven Rückmeldungen und der anhaltenden Nachfrage wird die Veranstaltungsreihe im Herbst 2026 im selben Format fortgeführt – mit denselben Referenten, aber mit aktualisierten Themen, die den weiteren Entwicklungen im Bereich KI Rechnung tragen.

Im Jahr 2025 setzte die DSS zudem einen neuen fachlichen Schwerpunkt im Bereich **Datenschutz und Datensicherheit im Gesundheitswesen**. Zwischen 23. Oktober und 25. November wurden insgesamt drei spezifische Fachveranstaltungen mit knapp 90 Teilnehmenden durchgeführt. Zwei Veranstaltungen fanden bei der LAK in Triesen statt, eine weitere richtete sich an Mitglieder der Liechtensteinischen Ärztekammer. Inhaltlich standen praxisrelevante Fragestellungen im Vordergrund, darunter der Umgang mit besonders schützenswerten Gesundheitsdaten, Zugriffs- und Berechtigungskonzepte, Datensicherheitsanforderungen sowie Meldepflichten bei Datenschutzverletzungen im medizinischen Kontext.

Den Teilnehmenden wurde im Vorfeld Gelegenheit zur Einreichung von Fragen gegeben, da es das Ziel war, eine praxisorientierte Veranstaltung durchzuführen. Das Interesse war gross und die DSS konnte zahlreiche Fragen beantworten. Die DSS bedankt sich bei den Teilnehmenden für ihr grosses Engagement.

1.2 Vorträge und Mitwirkung an Veranstaltungen

Zusätzlich zu den eigenen Veranstaltungen nahmen Mitarbeitende der DSS als Referentinnen bzw. Referenten an Informations- und Diskussionsveranstaltungen von externen Organisatoren teil.

1.2.1 Kooperation mit den Universitäten in Liechtenstein

Auch im Berichtsjahr war die Intention der DSS, schwerpunktmässig mit den beiden Universitäten in Liechtenstein zusammenzuarbeiten und gemeinsame Veranstaltungen anzubieten.

Am 27. November fand das **7. Fortbildungsseminar zur Datenschutz-Grundverordnung (DSGVO)** statt. Die etablierte Fachveranstaltung wurde in bewährter Zusammenarbeit mit der Privaten Universität im Fürstentum Liechtenstein (UFL), dem Datenschutzverein Liechtenstein, der Liechtensteinischen Industrie- und Handelskammer, BWBLEGAL, privacyofficers.at, der Data Privacy Community, dem Verein für Unternehmens-Datenschutz (VUD) sowie dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. durchgeführt.

Die Veranstaltung bot praxisorientierte Fachvorträge renommierter Expertinnen und Experten aus Liechtenstein, Deutschland, Österreich und der Schweiz. Im Zentrum standen aktuelle Entwicklungen in Rechtsprechung und (Aufsichts-)Praxis sowie deren konkrete Auswirkungen auf Unternehmen und öffentliche Stellen. Die DSS war als Mitveranstalterin auch aktiv in die Organisation sowie in die Themen- und Referentenauswahl eingebunden.

Der Vortrag der DSS widmete sich dem Auskunftsrecht gemäss Art. 15 DSGVO im Lichte der jüngeren Rechtsprechung des EuGH. Unter dem Leitgedanken «Auskunftsrecht – neu interpretiert durch den EuGH» wurden insbesondere das weitreichende Recht auf Kopie sowie das zentrale Erfordernis der Kontextualisierung der offengelegten Daten vertieft behandelt. Dabei wurde deutlich, dass eine pauschale oder abstrakte Beschreibung der verarbeiteten Daten regelmässig nicht (mehr) ausreicht, sondern konkrete und verständliche Informationen zur jeweiligen tatsächlichen Verarbeitungssituation bereitzustellen sind.

Das Fortbildungsseminar unterstrich erneut die Bedeutung kontinuierlicher Fortbildung im Datenschutzrecht. Angesichts dynamischer rechtlicher Ent-

wicklungen und einer zunehmend differenzierten Rechtsprechung bleibt der fachliche Austausch auf hohem Niveau ein wesentlicher Bestandteil wirksamer Compliance.

Darüber hinaus bot die DSS in Kooperation mit der UFL im Vorfeld des Fortbildungsseminars im Mai 2025 auch einen **Kurs Basiswissen Datenschutz** an. Ziel dieses Kurses war es, Einsteigerinnen und Einsteigern eine Möglichkeit zu bieten, Grundwissen im Bereich Datenschutz zu erwerben, um dann in einem Betrieb die Rolle des betrieblichen Datenschutzbeauftragten übernehmen zu können. Die DSS deckte in diesem Kurs sowohl die rechtliche als auch die technische Seite des Datenschutzes ab. Eine Neuerung in diesem Kurs war eine noch stärkere Praxisorientierung. Durch gezielte Übungen am Ende jeder Unterrichtseinheit erhielten die Teilnehmenden einen Einblick in die praktische Umsetzung der DSGVO und ein Gefühl für die kniffligen Fragen in der Praxis.

Ergänzt wurde dieser Basiskurs mit einem **Intensivkurs Datenschutzmanagement** von September bis Oktober 2025, der ebenfalls von der UFL in Kooperation mit der DSS und dem Datenschutzverein Liechtenstein angeboten wurde. Der Intensivkurs Datenschutzmanagement ist modular aufgebaut und verbindet fachliche Vertiefung mit praxisorientierter Anwendung.

Im ersten Modul vermitteln Expertinnen und Experten fundiertes Wissen zu zentralen Themen des Datenschutzes und der Datensicherheit. Die Teilnehmenden erhalten einen strukturierten Überblick über rechtliche Grundlagen, organisatorische Anforderungen sowie technische Schutzmassnahmen.

Im zweiten Modul steht die praktische Umsetzung im Vordergrund. Anhand konkreter Fallbeispiele und typischer Praxissituationen wird das erworbene Wissen gemeinsam analysiert, angewendet und vertieft. Ziel ist es, datenschutzrechtliche Fragestellungen systematisch zu erfassen und tragfähige Lösungen zu entwickeln.

Das dritte Modul umfasst die Teilnahme am Fortbildungsseminar zur Datenschutz-Grundverordnung.

Auf Einladung der **Universität Liechtenstein** übernahm die DSS im Berichtsjahr erneut jeweils mehrere Lehreinheiten zu rechtlichen und technischen Anforderungen des Datenschutzes in verschiedenen Weiterbildungs- und Studienprogrammen. Dazu zählten der Zertifikatsstudiengang Compliance-Officer, der Executive Master of Laws (LL.M.) im Bank- und Finanzmarktrecht, der Diplomstudiengang Treuhandwesen sowie Weiterbildungsformate im Versicherungswesen.

Die Lehrveranstaltungen waren jeweils zweigeteilt aufgebaut. Im ersten Teil wurden die rechtlichen Rahmenbedingungen und die praktische Umsetzung der DSGVO in Unternehmen bzw. Finanzintermediären behandelt. Dabei standen insbesondere Fragen der Rechtsgrundlagen, der Rechenschaftspflicht, der Betroffenenrechte sowie der organisatorischen Implementierung datenschutzkonformer Prozesse im Fokus.

Der zweite Teil widmete sich vertieft technischen und organisatorischen Aspekten. Thematisiert wurden unter anderem Anforderungen an die Datensicherheit, die Durchführung und Dokumentation von Datenschutz-Folgenabschätzungen, der Umgang mit Datenschutzverletzungen einschliesslich Meldepflichten sowie die Umsetzung der Prinzipien «Privacy by Design» und «Privacy by Default». Ergänzend wurden praxisrelevante Fragestellungen zum rechtskonformen Einsatz von Tracking-Technologien und zu einem datenschutzkonformen Cookie-Management behandelt.

1.2.2 Schulungen zu Datenschutz und Sozialen Medien

Im Auftrag des Elternbeirats der weiterführenden Schulen in Eschen fand im Mai 2025 ein **Informationsabend für die Eltern zum Thema «Medienerziehung im digitalen Zeitalter: Strategien für Eltern»** statt. Neben Vertretern der DSS gestalteten die Liechtensteinische Landespolizei, die Offene Jugendarbeit Eschen-Nendeln, die Fachgruppe Medienkompetenz sowie die Fachbereichsleiterin der Schulsozialarbeit die Veranstaltung mit. Im Impulsvortrag wurde der bewusste Umgang mit digitalen Medien thematisiert. Konkret wurden die Bedeutsamkeit von Medienkompetenz, Chancen und Risiken der Sozialen Medien sowie rechtliche Aspekte wie Strafmündigkeit und Datenschutz präsentiert. Im Anschluss an den Vortrag wurden im Podium Fragen und Erfahrungsberichte aus dem Publikum rege diskutiert.

Auf Anfrage der Fachgruppe Medienkompetenz beteiligte sich die DSS am 26. Februar an einem **Themenabend «Mentale Gesundheit» im Clinicum Alpinum**. Die DSS gestaltete gemeinsam mit der Stabsstelle Cyber-Sicherheit sowie der Schulsozialarbeit einen Impulsvortrag. Inhaltlich wurden die Bedeutung von Medienkompetenz im digitalen Alltag, insbesondere im Kontext psychischer Gesundheit, sowie Chancen und Risiken der Medien- und Smartphone-Nutzung beleuchtet. Dabei wurden sowohl entwicklungspsychologische als auch datenschutz- und sicherheitsrelevante Aspekte angesprochen. Anschliessend fand

eine Diskussion mit den Teilnehmenden statt, die auf grosses Interesse stiess. Besonders geschätzt wurden die praxisnahen Hinweise und konkreten Empfehlungen zum reflektierten Umgang mit Sozialen Medien und Smartphones.

1.2.3 Zentrum für Schulmedien – Weiterbildung Datenschutz/Datensicherheit für pädagogische Medienmentoren (PMM)

Am 26. März fand im Zentrum für Schulmedien in Vaduz ein Weiterbildungskurs zum Thema Datenschutz/Datensicherheit für die pädagogischen Medienmentoren des Schulamts (SA) statt. Der Kurs wurde vom SA in Kooperation mit der DSS abgehalten. Neben den grundlegenden Zielen und Prinzipien des Datenschutzrechts wurden auch die datenschutzrechtlichen Anforderungen bei der Prüfung von Softwareanträgen – insbesondere von digitalen Lehrmitteln – vertieft beleuchtet. Der Vortragsteil der DSS vermittelte die wesentlichen Grundlagen der Datensicherheit nach DSGVO, einschliesslich der technischen und organisatorischen Massnahmen (TOM) sowie der zugrunde liegenden Gewährleistungsziele. Abschliessend wurde diskutiert, wie Datensicherheit in der Praxis wirksam umgesetzt werden kann.

1.2.4 Interne Vorträge für die Mitarbeitenden der Landesverwaltung (LLV)

Wie in den Vorjahren bot die DSS im Rahmen der internen LLV-Weiterbildung erneut einen halbtägigen **Kurs zum Thema «Datenschutz»** an. Vermittelt wurden die rechtlichen Grundlagen des Schutzes des informationellen Selbstbestimmungsrechts sowie zentrale datenschutzrechtliche Prinzipien wie Rechtmässigkeit, Zweckbindung, Verhältnismässigkeit, Transparenz und Datensicherheit. Ergänzend wurden technische Aspekte des Datenschutzes behandelt. Im Fokus stand der datenschutzbewusste Umgang mit digitalen Endgeräten. Anhand von Webbrowsern, gängigen Smartphone-Betriebssystemen und häufig genutzten Apps wurden praxisnah Einstellungen aufgezeigt, mit denen sich der Schutz der Privatsphäre verbessern lässt. Abgerundet wurde der Kurs durch Hinweise zu weiterführenden Massnahmen, insbesondere zur Nutzung von Passwortmanagern, Zwei-Faktor-Authentifizierung (2FA), VPN-Diensten sowie zu einem insgesamt sparsamen und reflektierten Umgang mit personenbezogenen Daten.

Ebenfalls leistete die DSS mit einem **Webinar zum Thema «Ethik und KI in der Verwaltung»** einen fachlichen Beitrag zur LLV-Akademie. Die KI-Verordnung der EU verankert ethische Prinzipien wie Transparenz, Nicht-Diskriminierung, Sicherheit und Grundrechtsschutz in einem risikobasierten Regulierungsansatz. In der öffentlichen Verwaltung bedeutet dies, KI verantwortungsvoll, transparent und menschenzentriert einzusetzen, um Vertrauen und demokratische Werte zu sichern. Das Fazit und die zentrale Handlungsempfehlung an die Mitarbeitenden der LLV war, dass der verantwortungsvolle Einsatz von KI nicht allein durch rechtliche Regeln sichergestellt wird, sondern massgeblich vom individuellen Handeln abhängt. Jede und jeder Einzelne trägt Verantwortung dafür, KI reflektiert, transparent und menschenzentriert einzusetzen. Dazu gehört, den Einsatz von KI kritisch zu hinterfragen, ihre Rolle offen zu kommunizieren, ihre Grenzen klar zu erkennen und die Letztverantwortung für Entscheidungen beim Menschen zu belassen. Ebenso wesentlich sind ein grundlegendes Verständnis der gesellschaftlichen und rechtlichen Auswirkungen von KI sowie der Mut, ethische Bedenken anzusprechen.

1.2.5 Weitere Vorträge

Darüber hinaus engagierten sich die Mitarbeitenden der DSS im Berichtsjahr bei insgesamt dreizehn weiteren Informations- und Diskussionsveranstaltungen.

Innerhalb Liechtensteins gab die DSS eine Präsentation zur KI-Verordnung am Liechtenstein-Institut und hielt Vorträge mit einem Update zu den Datenschutzanforderungen beim Unternehmeranlass der Gemeinde Eschen-Nendeln, dem Aus- und Weiterbildungstag des Pensionskassenverbandes sowie dem Datenschutzverein. Ebenso hielt die DSS einen Vortrag zum Thema «Update Datenschutz: Rechte und Pflichten für Vereine» als Teil einer Weiterbildung für Vereine in der Erwachsenenbildung Stein Egerta.

Im nahen Ausland nahm die DSS erneut an einer Fachveranstaltung in Zürich für betriebliche Datenschutzexpertinnen und -experten aus der Schweiz teil und stellte dort ihre Perspektiven zu aktuellen regulatorischen und aufsichtsrechtlichen Entwicklungen dar. Darüber hinaus war die DSS mit eigenen Fachbeiträgen beim Privacy Ring in Luzern, bei der Jahrestagung 2025 der Datenschutzbeauftragten der öffentlichen Verwaltung Österreichs in Innsbruck, beim Schulthess Forum Data Privacy 2025 in Zürich sowie im Rahmen eines Roundtable für Studierende des CAS Datenschutz der Universität Zürich vertreten.

Inhaltlich befassten sich die Vorträge mit aktuellen Fragestellungen des Datenschutzrechts, einschlägiger Rechtsprechung sowie zunehmend mit den neuen Digitalisierungsrechtsakten der EU – insbesondere deren systematischem Zusammenspiel mit der DSGVO. Dabei standen Fragen der Kohärenz, Abgren-

zung und praktischen Umsetzung im Unternehmens- und Verwaltungsalltag im Mittelpunkt.

Diese breit gefächerten Aktivitäten unterstreichen die Rolle der DSS als fachliche Ansprechpartnerin über die Landesgrenzen hinaus. Zugleich leisten sie einen wichtigen Beitrag zur Sensibilisierung von Fachkreisen und Öffentlichkeit für die rechtlichen, technischen und organisatorischen Herausforderungen eines zunehmend komplexen europäischen Datenschutz- und Digitalrechtsrahmens.

1.3 Internetseite

Zwei zentrale Säulen der Öffentlichkeitsarbeit der DSS sind der Internetauftritt und der im Berichtsjahr sechzehn Mal versandte Newsletter. Beide Elemente sind miteinander verbunden, indem der Newsletter jeweils einen kurzen Überblick zu einem Thema gibt und zugleich auf weiterführende Informationen auf der Internetseite verweist. Diese integrierte Herangehensweise ermöglicht es den Empfängern, sich über den Newsletter hinaus nachgängig tiefergehend mit den präsentierten Themen auseinanderzusetzen.

Im Berichtsjahr verzeichnete die Internetseite zwar eine leichte Abnahme der Zugriffe, diese blieben jedoch insgesamt auf einem hohen Niveau. Dies unterstreicht nicht nur die Relevanz der von der DSS bereitgestellten Informationen, sondern auch die konstante Nachfrage nach qualitativ hochwertigen Ressourcen im Bereich Datenschutz. Die rege Nutzung beider Kanäle – Internetseite und Newsletter – zeigt die erfolgreiche Strategie der DSS, sowohl regelmässig aktuelle Informationen zu liefern als auch auf weiterführende Inhalte aufmerksam zu machen.

Die meisten Zugriffe auf die Internetseite betreffend die verschiedenen Themen unter der Rubrik «Datenschutz / Themen A–Z» wurden bei folgenden Beiträgen verzeichnet: Berechtigtes Interesse, besondere Datenkategorien nach Art. 9 und 10 DSGVO, Informationspflicht nach Art. 13 und 14 DSGVO, Schwärzen von Dokumenten und Bildern sowie Löschrecht und Löschpflicht.

1.4 Newsletter

Ende 2025 hatten 1'175 Personen den Newsletter der DSS abonniert und das Interesse daran bleibt weiterhin hoch. Im Berichtsjahr hat die DSS insgesamt 24 neue Informationsbeiträge und Veranstaltungsankündigungen auf ihrer Internetseite veröffentlicht und dazu 16 Newsletter versandt. Die drei meistgelesenen Newsletter 2025 waren jener zum KI-Training durch Meta, Aktuelles aus der Datenschutzstelle #5, sowie KI-Training durch LinkedIn.

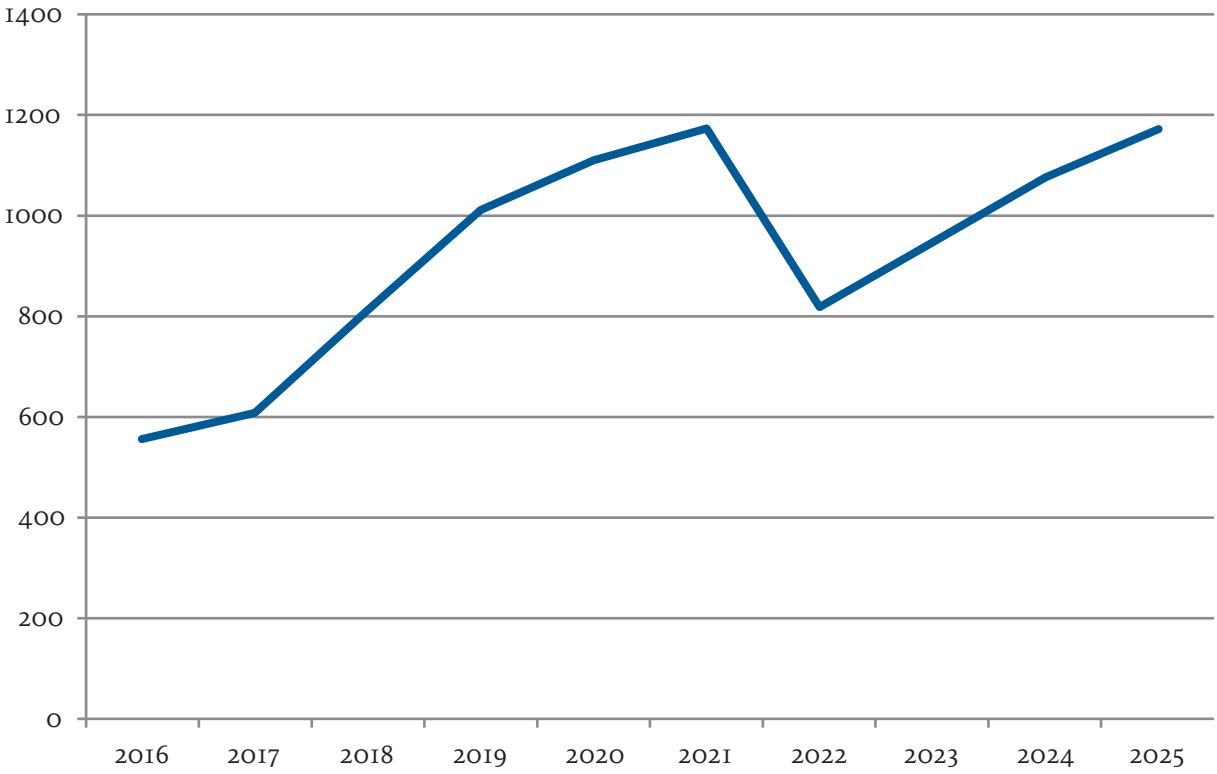


Abbildung 1: Entwicklung Newsletter-Abonnentinnen und Abonnenten

Sämtliche Newsletter können jederzeit auf der Internetseite der DSS nachgelesen werden. Ausserdem finden sich viele Inhalte der Newsletter dort auch in ausführlicher Form im Bereich «Themen A-Z» wieder. Nachdem bei jeder bedeutenden inhaltlichen Änderung oder Neuerung auf der Internetseite der DSS ein Newsletter versandt wird, bleiben die Newsletter-Abonnentinnen und -Abonnenten immer auf dem Laufenden, auch ohne die Internetseite in regelmässigen Abständen besuchen und auf Neuigkeiten hin überprüfen zu müssen.

Anregungen der Leserinnen und Leser zu neuen Themen für den Newsletter sind jederzeit willkommen und werden soweit möglich aufgenommen und umgesetzt.

1.5 Datenschutz in den Medien

Im Berichtsjahr war das Thema Datenschutz erneut regelmässig in den liechtensteinischen Medien präsent. Mit knapp 30 Beiträgen bewegte sich die Berichterstattung quantitativ auf einem ähnlichen Niveau wie im Vorjahr. Inhaltlich lag der Schwerpunkt der Printmedien insbesondere auf Fragen der fortschreitenden Digitalisierung und dem Einsatz von KI, auf datenschutzrechtlichen Herausforderungen im Bildungsbereich sowie auf der Thematik der Akteneinsicht im Zusammenhang mit dem Erzbistum Vaduz. Die mediale Aufmerksamkeit verdeutlicht, dass Datenschutzfragen zunehmend gesellschaftspolitische Relevanz besitzen und über den rein juristischen und technischen Kontext hinaus öffentlich diskutiert werden. Die mediale Berichterstattung zu datenschutzrechtlichen Themen und ihre positive Haltung gegenüber diesem Bereich leisten einen wertvollen Beitrag zur Umsetzung des kommunikativen Konzepts im Wissenstransfer. Dadurch werden auch Privatpersonen erreicht, die beruflich weniger mit Datenschutz in Berührung kommen und die auf diese Weise ebenfalls einen verständlichen Zugang zu dieser Materie erhalten.

«Über die letzten vier Jahre hinweg lässt sich ein klarer Trend zur steigenden Komplexität der Anfragen erkennen, der sich auch 2025 fortsetzte.»

2. Beratung zu konkreten Anfragen

2.1 Allgemeines

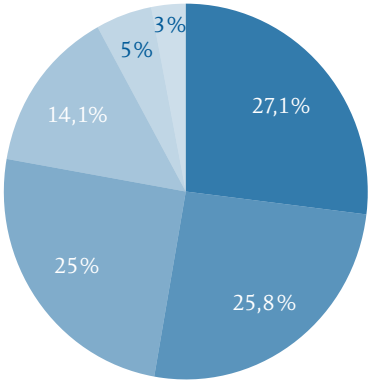
Im Berichtsjahr bearbeitete die DSS insgesamt 1'563 Anfragen von öffentlichen und privaten Institutionen sowie von Privatpersonen. Im Vergleich zu den 1'521 Anfragen des Vorjahres entspricht dies einem leichten Anstieg um 2,8 %. Über die letzten vier Jahre hinweg lässt sich jedoch ein klarer Trend zur steigenden Komplexität der Anfragen erkennen, der sich auch 2025 fortsetzte.

Die fortschreitende technologische Entwicklung führte zu einer Vielzahl neuer und anspruchsvoller Fragestellungen, insbesondere im Hinblick darauf, ob und wie technische Systeme die Anforderungen des Datenschutzes erfüllen können. Besonders der Einsatz von KI sorgte erneut für zahlreiche Anfragen von Verantwortlichen. Ein weiterer Beratungsschwerpunkt lag auch im Berichtsjahr wieder auf der Nutzung von Videoüberwachungen durch private und kommerzielle Akteure.

Ergänzend rückte die Frage der datenschutzrechtlichen Zulässigkeit und praktischen Ausgestaltung von Cloud-Lösungen verstärkt in den Fokus. Zahlreiche öffentliche Stellen und Unternehmen prüften im Berichtsjahr die Auslagerung von Datenverarbeitungen an grosse internationale Cloud-Dienstleister. Dabei stellten sich komplexe Fragen zur Rollenverteilung zwischen Verantwortlichem und Auftragsverarbeiter, zu geeigneten Garantien bei Drittstaatentransfers sowie zur vertraglichen und technischen Absicherung gemäss der DSGVO. Neben den Vorteilen solcher Lösungen – etwa Skalierbarkeit, hohe Sicherheitsstandards und professionelle Betriebsstrukturen – waren auch Risiken wie Abhängigkeiten von einzelnen Anbietern, eingeschränkte Kontrollmöglichkeiten und die Transparenz von Datenflüssen sorgfältig zu bewerten. Eine besondere Herausforderung in der Beratungspraxis bestand darin, dass die DSS weder einzelne Produkte noch konkrete Cloud-Dienstleister bewerten oder empfehlen kann. Aufgrund ihres gesetzlichen Mandats und ihrer institutionellen Unabhängigkeit ist es der Aufsichtsbehörde verwehrt, Marktakteure zu zertifizieren oder bestimmte Lösungen als «datenschutzkonform» freizugeben.

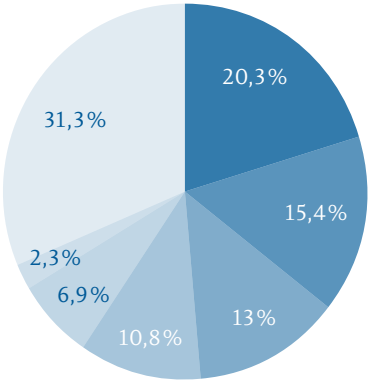
Hinzu kam, dass die datenschutzrechtliche Beurteilung von Cloud-Nutzungen regelmässig nicht abstrakt, sondern nur auf Grundlage der jeweils konkret gewählten Konfiguration, der vertraglichen Ausgestaltung sowie der getroffenen technischen und organisatorischen Massnahmen erfolgen kann. Aspekte wie Speicherort, Verschlüsselung, Zugriffs- und Berechtigungskonzepte, Protokollierung, Unterauftragsverhältnisse oder internationale Datenflüsse beeinflussen die rechtliche Bewertung wesentlich. Viele Fragestellungen liessen sich daher nur einzelfallbezo-

Wer stellt die Fragen?



- Internationales
- Öffentliche Hand
- Privatwirtschaft
- Privatpersonen
- Vereine und Stiftungen
- Medien

Verteilung der Anfragen aus der Privatwirtschaft



- Finanzintermediäre
- IT und Telekommunikation
- Anwaltskanzleien
- Industrie
- Versicherungen
- Gesundheitswesen
- Andere

gen beantworten und erforderten von den Verantwortlichen eine sorgfältige, dokumentierte Risikoanalyse im Sinne der Rechenschaftspflicht gemäss der DSGVO.

Weitere aktuelle Themen des Jahres 2025 betrafen die rechtssichere Ausgestaltung von Tracking- und Cookie-Mechanismen, den Umgang mit vermehrten Cyberangriffen und Phishing-Vorfällen sowie die Abgrenzung zwischen Pseudonymisierung und Anonymisierung im Lichte aktueller europäischer Rechtsprechung. Auch die Anforderungen an Transparenz, Dokumentation und Rechenschaftspflicht bei automatisierten Entscheidungsprozessen gewannen weiter an Bedeutung. Insgesamt zeigte sich, dass technische Innovationen zunehmend eine vertiefte rechtliche und technische Analyse erfordern und die DSS sowohl beratend als auch aufsichtsrechtlich in komplexen digitalen Transformationsprozessen gefordert war.

Die Herkunft der Anfragen zeigt ein vielfältiges Bild: Jeweils rund ein Viertel der Anfragen stammte aus dem internationalen bzw. EU/EWR-Raum (27,1 %), dem öffentlichen Sektor (25,8 %) sowie der Privatwirtschaft (25,0 %). Der Grossteil der Anfragen aus dem privaten Sektor kam von Kleinen und Mittleren Betrieben (KMU) verschiedener Branchen, gefolgt von Finanzintermediären, der IT und Telekom-Branche sowie von Anwaltskanzleien. Der Anteil von Privatpersonen, die Anfragen an die DSS stellten, hat mit 14,1 % leicht abgenommen. Anfragen von Vereinen und Stiftungen sind ebenfalls leicht zurückgegangen (5,0 %), während sich die Anfragen von Medien 2025 verdoppelt haben (3,0 %).

Diese Zahlen verdeutlichen die wachsende Bedeutung datenschutzrechtlicher Themen in unterschiedlichsten Bereichen. Gleichzeitig zeigen sie, wie eng Liechtenstein als EWR-Mitgliedstaat in die europäische Datenschutz- und Digitalisierungsagenda eingebunden ist und welch zentrale Rolle der DSS bei der Unterstützung und Information der betroffenen Akteure zukommt.

Beratungsanfragen konnten telefonisch, schriftlich – insbesondere mittels E-Mail – oder auch in einem persönlichen Gespräch bei der DSS eingebracht werden.

Ganz allgemein stellte sich auch im Berichtsjahr wieder die Frage, ob und in welchem Ausmass eine Datenschutz-Aufsichtsbehörde überhaupt beratend tätig sein sollte bzw. ob Aufsicht durch Beratung überhaupt im Sinne der DSGVO ist. Die DSS blieb bei ihrer grundsätzlichen Auffassung, dass Beratung ein zentrales Element der Umsetzung der Datenschutzbestimmungen darstellt. So ist es zwar korrekt, dass die Beratung von Verantwortlichen und Auftragsverarbeitern weder in der DSGVO noch im liechtensteinischen Datenschutzgesetz (DSG) als explizite Aufgabe der Aufsichtsbehörden erwähnt wird, allerdings lässt sie sich als Teil von Art. 57 Abs. 1 Bst. v DSGVO verstehen, wonach die Aufsichtsbehörde «jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen kann».

Vor dem Hintergrund der aktuell begrenzten personellen Ressourcen sowie einer stetigen Zunahme komplexer Aufgaben – insbesondere im Zusammenhang mit neuen technologischen Entwicklungen – müsste diese auf Eigeninitiative beruhende Beratungstätigkeit im Falle weiterer Ressourcenverknappung allerdings überprüft und gegebenenfalls

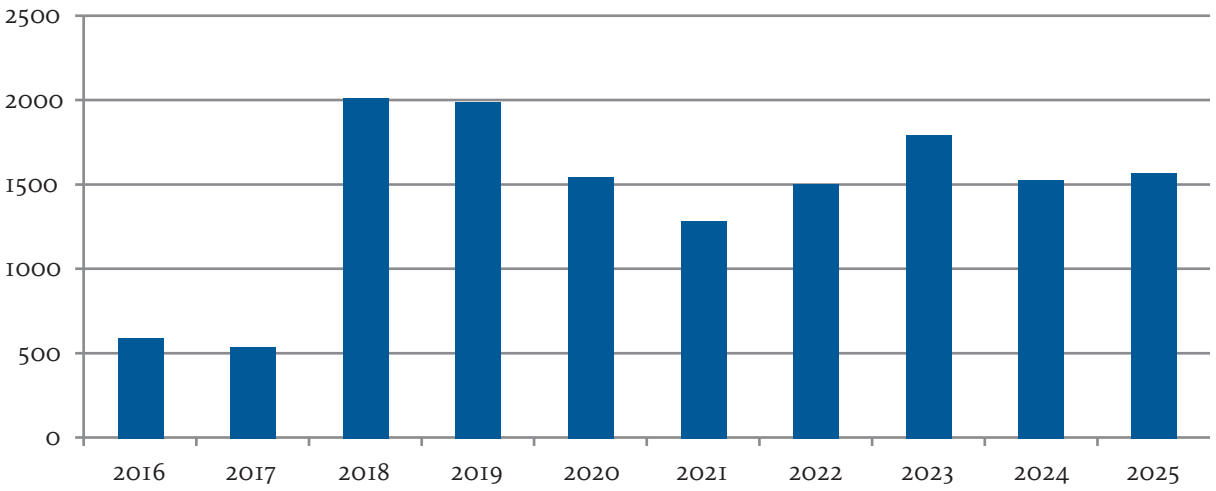


Abbildung 2: Anzahl Anfragen pro Jahr

reduziert werden. Auf die personellen Rahmenbedingungen und deren Auswirkungen auf die Aufgabenwahrnehmung wird im Kapitel «Interne Organisation» näher eingegangen.

Heikel ist die Frage der Beratung durch die DSS jedoch in einem laufenden Beschwerdeverfahren gemäss Art. 57 Abs. 1 Bst. f DSGVO oder während einer amtswegigen Untersuchung gemäss Art. 57 Abs. 1 Bst. h DSGVO. Die DSS hält in Bezug auf diese spezielle Fallkonstellation deshalb eine ganz klare Trennung zwischen ihren Beratungsaufgaben und ihrer Aufsichtstätigkeit für unumgänglich. Sobald die DSS von ihren Untersuchungsbefugnissen gemäss Art. 58 Abs. 1 DSGVO Gebrauch macht, ist eine Beratung nicht mehr möglich und die Kommunikation mit den Verantwortlichen hat sich auf die Durchführung der Untersuchung bzw. die Erfüllung von Anordnungen der DSS in diesem Zusammenhang zu beschränken. Es kann zwar eine Anleitung zur Erfüllung der Anweisungen gegeben werden, nicht jedoch eine umfassende Rechtsberatung, wie sie bei einer reinen Anfrage einer öffentlichen oder privaten Stelle möglich wäre.

Bereits im Jahr 2023 hat die DSS ihre Strategie zur klaren Abgrenzung zwischen aufsichtsrechtlicher Untersuchung und beratender Tätigkeit punktuell weiterentwickelt. Seither bietet sie – auf Wunsch der verantwortlichen Stelle – gezielte Beratungstermine zur Umsetzung rechtskräftiger Verfügungen an. Ziel dieser Anpassung ist es, nach Abschluss des formellen Verfahrens eine sachgerechte und effiziente Umsetzung der angeordneten Massnahmen zu unterstützen, ohne die institutionelle Trennung zwischen Kontrolle und Beratung aufzugeben.

Im Berichtsjahr bestätigte sich erneut die Zweckmässigkeit dieses Vorgehens. Durch die strukturierte Begleitung im Anschluss an eine Verfügung konnten offene Umsetzungsfragen frühzeitig geklärt, Missverständnisse vermieden und Verzögerungen reduziert werden. Dies führte in mehreren Fällen zu einer deutlich beschleunigten Herstellung eines datenschutzkonformen Zustands und trug zugleich zur Rechtssicherheit der betroffenen Organisationen bei.

2.2 Videoüberwachung und Veröffentlichung von Bildmaterial

Seit Inkrafttreten der DSGVO hebt die DSS in jedem Tätigkeitsbericht hervor, dass Videoüberwachungen einen dauerhaften Schwerpunkt ihrer Aufsichtstätigkeit bilden. Dies traf auch im Berichtsjahr zu. Angesichts der fortschreitenden technischen Entwicklungen bleibt festzuhalten, dass Videoüberwachung ein datenschutzrechtliches Kernthema bleibt, solange entsprechende Systeme eingesetzt werden. Im Berichtsjahr zeigte sich abermals, dass neue technische Lösungen und Einsatzformen auf den Markt gelangen und bestehende Überwachungspraktiken verändern.

Ein erkennbarer Trend betraf die Videoüberwachung von Baustellen. Die DSS erhielt Anfragen sowohl zur Dokumentation des Baufortschritts als auch zur Kontrolle der Arbeitsleistung im Zusammenhang mit Abrechnungen. Während die rein technische Erfassung des Baufortschritts grundsätzlich ohne Verarbeitung personenbezogener Daten möglich ist, wirft die Leistungsüberwachung von Arbeitnehmenden erhebliche datenschutzrechtliche Fragen auf. Für beide Zwecke ist die Verarbeitung personenbezogener Daten grundsätzlich nicht erforderlich, da der Baufortschritt oder Materialbestände etc. auch ohne Identifizierbarkeit einzelner Personen dokumentiert werden können. Technische Lösungen, die Personen automatisiert aus dem Bildmaterial entfernen oder verpixeln, lösen das datenschutzrechtliche Problem jedoch nicht vollständig, da bereits dieser Anonymisierungsprozess eine Datenverarbeitung darstellt. Werden zudem Rohdaten gespeichert, die noch identifizierbare Personen enthalten, bestehen weiterhin erhebliche rechtliche Anforderungen, insbesondere hinsichtlich Rechtsgrundlage, Zweckbindung, Speicherbegrenzung und Zugriffskontrolle. Die DSS prüft entsprechende Vorhaben vertieft, sobald sie konkret umgesetzt werden sollen.

Ein weiterer Schwerpunkt lag auf Videoüberwachungen in Wohnbereichen. Während entsprechende Fragestellungen im nachbarschaftlichen Kontext seit Jahren auftreten, verzeichnete die DSS im Berichtsjahr einen deutlichen Anstieg von Anfragen zu Videoüberwachungen in Mehrfamilienhäusern. Betroffen waren insbesondere Garagen, Abfallräume, Hauseingänge sowie allgemein zugängliche Innenbereiche. Die datenschutzrechtliche Beurteilung orientiert sich grundsätzlich an denselben Kriterien wie bei Einfamilienhäusern. Als Rechtsgrundlage kommt entweder eine Einwilligung oder ein berechtigtes Interesse in Betracht. In Wohnbereichen lässt sich ein berechtigtes Interesse allerdings regelmässig nicht ausreichend begründen, da das Schutzinteresse der anderen Bewohner und Besucher überwiegt. Praktisch verbleibt daher nur die Einwilligung sämtlicher betroffener Bewohner. Diese muss freiwillig, informiert und jederzeit widerrufbar sein und darf nicht an vertragliche Verpflichtungen – etwa einen Mietvertrag – gekoppelt werden. In der Praxis führt dies zu erheblichen Umsetzungsproblemen, da bereits der Widerruf durch eine einzelne Person die Abschaltung der Anlage erforderlich macht.

Auch im nachbarschaftlichen Umfeld von Einfamilienhäusern blieb die DSS beratend tätig. Besonders hervorzuheben sind zwei Fälle, in denen sich betroffene Nachbarn aufgrund eines von der DSS bereitgestellten Musterschreibens eigenständig meldeten. Dieses Schreiben steht seit mehreren Jahren auf der Internetseite der DSS zur Verfügung und ermöglicht es Nachbarn, anonym oder offen auf eine potenziell unzulässige Videoüberwachung hinzuweisen und ermutigt zur Kontaktaufnahme mit der DSS. Dieses niederschwellige Instrument trägt dazu bei, eskalierende Nachbarschaftskonflikte zu vermeiden und datenschutzkonforme Lösungen im Dialog zu erreichen.

Im Bereich Hotellerie und Gastronomie setzte die DSS ihre Beratungstätigkeit zu Videoüberwachungen ebenfalls fort. Bereits im Vorjahr hatte sie zur Videoüberwachung in einem Hotel Stellung genommen und klargestellt, dass Gäste in Bereichen der Freizeitgestaltung nicht überwacht werden dürfen. Die Überwachung von Lobby- oder Aufenthaltsräumen ist somit unzulässig. Im Berichtsjahr prüfte die DSS weitere Konstellationen. Massgeblich sind jeweils der konkrete Zweck, der Kreis der betroffenen Personen und die Eingriffsintensität. So ist etwa die Überwachung eines nicht öffentlich zugänglichen Weinkellers zulässig, während eine Überwachung des Restaurationsbetriebs unzulässig ist. Für Hotelgänge reicht ein berechtigtes Interesse grundsätzlich nicht aus, wohingegen Eingangsbereiche oder Tiefgaragen unter bestimmten Voraussetzungen überwacht werden dürfen.

Ein weiterer Fall betraf die Videoüberwachung eines Spielplatzes. Geprüft wurde die Erfassung des Bereichs vor WC-Anlagen, des Holzlagers sowie des Spielplatzes selbst. Aufgrund wiederholter Vorkommnisse von Vandalismus wurde eine Kameraüberwachung unmittelbar vor den WC-Anlagen als zulässig beurteilt. Unter Berücksichtigung der Rechtsprechung des Verwaltungsgerichtshofs (VGH 2022/109) ist auch die Überwachung eines Holzlagers zur Durchsetzung eines Feuerverbots und zum Schutz vor Sachbeschädigung zulässig. Dagegen ist die flächendeckende Überwachung des Spielplatzes mit dem berechtigten Interesse der Besucher und Besucherinnen an einer unbeobachteten Freizeitgestaltung nicht vereinbar. Als milderes Mittel kommt eine rein technische Live-Übersicht ohne Speicherung personenbezogener Daten in Betracht.

Darüber hinaus befasste sich die DSS mit Videoüberwachungen innerhalb privater Wohnräume. Solche Systeme fallen nicht unter die Haushaltsausnahme, wenn sie Zwecken wie Sicherheit oder Kontrolle gegenüber Dritten dienen. Besonders problematisch ist der Einsatz von Kameras gegenüber Mitarbeitenden oder externen Dienstleistern wie etwa Reinigungs- oder Pflegepersonal, da dies eine Form der Arbeitsplatzüberwachung darstellt. Diese ist nur unter äusserst restriktiven Voraussetzungen zulässig. Eine Einwilligung scheidet regelmässig ebenfalls aus, da davon ausgegangen werden kann, dass sie im Arbeitsverhältnis nicht freiwillig erteilt wird. Die Relevanz dieses Themas zeigte sich auch im europäischen Kontext: Im Rahmen eines behördlichen Austauschs wurde eine vergleichbare Fragestellung aus einem anderen EU-Staat an die DSS herangetragen.

Neben privaten Haushalten und Gastronomiebetrieben beriet die DSS auch Unternehmen, Detailhandelsgeschäfte, eine Tankstelle sowie Behörden zu geplanten oder bestehenden Videoüberwachungen.

Im letzten Tätigkeitsbericht informierte die DSS über die Eröffnung einer datenschutzrechtlichen Überprüfung der Videoüberwachung der Landespolizei in Schaan. Die DSS war bereits im Vorfeld der Umsetzung beratend eingebunden. Angesichts der besonderen Grundrechtssensibilität stationärer Videoüberwachung im öffentlichen Raum entschied sie sich dann zusätzlich für eine eigenständige, vertiefte aufsichtsrechtliche Prüfung. Die umfassende technische und rechtliche Analyse ergab, dass die Landespolizei insgesamt um eine datenschutzkonforme Ausgestaltung bemüht ist und zahlreiche Schutzmassnahmen implementiert hat. Gleichwohl identifizierte die DSS mehrere Punkte mit Anpassungsbedarf, deren Umsetzung im Folgejahr vorgenommen wird.

Die Überprüfung zeigte insbesondere, dass trotz umfangreicher Massnahmen zur Verpixelung aufgrund der hohen Bildauflösung sowie der vorhandenen Zoom- und Schwenkfunktionen private Liegenschaften, namentlich Häuser und Wohnungen, erfasst werden konnten. Darüber hinaus gerieten auch Bereiche ins Sichtfeld der Kameras, die der Freizeitgestaltung sowie dem sozialen und kulturellen Austausch dienen, insbesondere Gastronomiebetriebe. Eine solche Erfassung steht nicht im Einklang mit den gesetzlichen Vorgaben und den datenschutz- sowie grundrechtlichen Anforderungen an die Verhältnismässigkeit und Zweckbindung der Überwachung.

Ferner stellte die DSS Defizite bei der Erfüllung der Informationspflichten fest. Im Rahmen der Sachverhaltsermittlung führte sie als ergänzendes Element eine nicht repräsentative Vor-Ort-Befragung von Passanten durch. Diese ergab, dass die Verantwortlichkeit für die Videoüberwachung für Betroffene nicht klar erkennbar war. Zudem wusste keine der befragten Personen, dass die Kameras am Lindaplatz standardmässig nicht aufzeichnen. Auch die auf der Internetseite der Landespolizei bereitgestellten Informationen wiesen

punktuelle Transparenzmängel auf und bedurften einer Präzisierung.

Insgesamt gingen im Berichtsjahr 21 Meldungen über neu installierte stationäre Videoanlagen sowie vier Meldungen über Drohnenflüge mit Kameras bei der DSS ein.

2.3 Verbindliche interne Datenschutzvorschriften

Im Berichtsjahr stellte die internationale Datenübermittlung erneut einen thematischen Schwerpunkt der Beratungstätigkeit dar. Wie bereits im Vorjahr ausgeführt, bilden verbindliche interne Datenschutzvorschriften (Binding Corporate Rules; BCR) eines der in Kapitel V der DSGVO vorgesehenen Instrumente zur rechtlichen Absicherung von Übermittlungen personenbezogener Daten in Drittländer. Sie richten sich speziell an international tätige Unternehmen bzw. Unternehmensgruppen und schaffen für diese ein verbindliches, konzernweit einheitliches Datenschutzregelwerk, wenn im Rahmen von Datenverarbeitungen personenbezogene Daten aus dem EU/EWR-Raum in Drittländer gelangen. BCR ermöglichen eine strukturierte und langfristig tragfähige Lösung für konzerninterne Datentransfers, da sie organisationsweit gelten und jederzeit an gesetzliche sowie technologische Entwicklungen angepasst werden können.

BCR wurden bereits vor Inkrafttreten der DSGVO als aufsichtsbehördlich anerkanntes Instrument für internationale Datenübermittlungen in Drittstaaten entwickelt und mit der DSGVO sodann ausdrücklich normiert und inhaltlich konkretisiert. Ihre Genehmigung erfolgt im Kohärenzverfahren: Die federführende Aufsichtsbehörde prüft den Antrag eines Unternehmens in enger Abstimmung mit anderen europäischen Datenschutz-Aufsichtsbehörden; zudem ist der Europäische Datenschutzausschuss (EDSA) in das Verfahren eingebunden.

Wie im letzten Tätigkeitsbericht angekündigt, initiierte die DSS im Berichtsjahr ein neues BCR-Genehmigungsverfahren als federführende Aufsichtsbehörde. Im Rahmen dieses Verfahrens fanden zunächst mehrere Vorabklärungen und Beratungsgespräche statt. Gegen Ende des Berichtsjahres reichte das antragstellende liechtensteinische Unternehmen einen ersten umfassenden Entwurf der BCR-Dokumentation ein. Die inhaltliche Prüfung, die Abstimmung mit den europäischen Partnerbehörden sowie die weitere begleitende Beratung durch die DSS werden im 2026 fortgesetzt.

2.4 Auswahl konkreter rechtlicher Fragen

Die DSS hat im Berichtsjahr wieder zahlreiche Anfragen zur Klärung und Beurteilung von datenschutzrechtlichen Fragestellungen erhalten. Einige davon, vor allem solche, die mehrfach gestellt wurden und allgemein beantwortet werden konnten, werden nachfolgend kurz dargestellt.

Datenschutz nach dem Tod

Im Berichtsjahr wurde die DSS wiederholt mit der Frage konfrontiert, ob und unter welchen Voraussetzungen Auskünfte über personenbezogene Daten verstorbener Personen verlangt werden können. In ihrer Beratung stellte die DSS klar, dass die DSGVO gemäss Erwägungsgrund 27 nicht für personenbezogene Daten Verstorbener gilt. Zwar eröffnet der Erwägungsgrund den Mitgliedstaaten die Möglichkeit, nationale Regelungen für den Umgang mit Daten Verstorbener vorzusehen; Liechtenstein hat von dieser Option im DSG jedoch keinen Gebrauch gemacht. Der datenschutzrechtliche Schutz bezieht sich somit ausschliesslich auf lebende natürliche Personen – mit dem Tod endet die Anwendbarkeit des Datenschutzrechts.

Auskünfte nach dem Tod einer Person können sich daher nicht auf Art. 15 DSGVO stützen, sondern müssen gegebenenfalls auf andere Rechtsgrundlagen gestützt werden. In Betracht kommen etwa zivilrechtliche Ansprüche, erbrechtliche Konstellationen oder spezifische vertragliche bzw. regulatorische Bestimmungen einzelner Branchen (z.B. Banken oder Versicherungen). Zu berücksichtigen ist zudem, dass bestimmte Berufsgeheimnisse oder Verschwiegenheitspflichten – anders als der Datenschutz – über den Tod hinaus fortwirken können. Auch Fragen der Form und Sicherheit der Übermittlung richten sich in solchen Fällen nicht mehr nach der DSGVO. Weiterführende Hinweise stellt die DSS auf ihrer Internetseite unter dem Titel «Spezialfall: Auskunft über personenbezogene Daten verstorbener Personen» zur Verfügung.

Zulässigkeit von personenbezogenen Daten in der Betreff-Zeile eines E-Mails

Ob personenbezogene Daten in der Betreffzeile einer E-Mail verwendet werden dürfen, ist nach den Grundsätzen der Datenminimierung und Vertraulichkeit gemäss Art. 5 Abs. 1 Bst. c und f DSGVO zu beurteilen. Da Betreffzeilen häufig bereits in der Vorschau sichtbar sind – etwa auf Sperrbildschirmen – besteht ein erhöhtes Risiko unbefugter Kenntnisnahme. Hinzu kommt, dass Betreffzeilen aus technischer Sicht regelmässig nicht oder nur eingeschränkt Ende-zu-Ende-verschlüsselt sind und als Metadaten in Mailservern, Logfiles oder Backups verarbeitet werden. Sie sind daher strukturell weniger geschützt als

der eigentliche Nachrichteninhalt. Personenbezogene Daten dürfen folglich nur unter sehr engen Voraussetzungen in der Betreffzeile erscheinen, etwa wenn sie für den Kommunikationszweck unabdingbar sind und kein besonderes Schutzbedürfnis besteht. Sensible Daten, insbesondere solche im Sinne von Art. 9 DSGVO, dürfen dort grundsätzlich nicht genannt werden. Im Zweifel ist eine neutrale Formulierung zu wählen und detaillierte Informationen sind im E-Mail-Text selbst – gegebenenfalls unter Einsatz geeigneter Schutzmassnahmen – zu übermitteln.

Einrichtung einer Abwesenheitsnotiz durch den Arbeitgeber

Mehrmals gelangten Verantwortliche mit der Frage an die DSS, ob ein Arbeitgeber bei unvorhergesehener Krankheit oder sonstiger kurzfristiger Abwesenheit eines Mitarbeitenden eigenständig eine Abwesenheitsnotiz im geschäftlichen E-Mail-Postfach einrichten darf.

Die DSS stellte klar, dass dies grundsätzlich zulässig sein kann, sofern die Verarbeitung auf berechtigte Interessen des Arbeitgebers im Sinne von Art. 6 Abs. 1 Bst. f DSGVO gestützt werden kann. Ein solches Interesse liegt insbesondere in der Aufrechterhaltung des Geschäftsbetriebs und der Sicherstellung einer geordneten externen Kommunikation. Für die Interessenabwägung mit allfälligen schutzwürdigen Interessen der betroffenen Person ist wesentlich, ob die private Nutzung des geschäftlichen E-Mail-Kontos untersagt oder zumindest stark eingeschränkt ist. Je geringer die Wahrscheinlichkeit privater Inhalte, desto eher überwiegt das berechtigte Interesse des Arbeitgebers. Die Umsetzung sollte zudem verhältnismässig erfolgen, nach Möglichkeit im Vier-Augen-Prinzip und – sofern vorhanden – unter Einbezug der oder des Datenschutzbeauftragten.

Anbieter bzw. Betreiber eines KI-Tools als Auftragsverarbeiter oder eigener Verantwortlicher

Ob ein Anbieter oder Betreiber eines KI-Tools als Auftragsverarbeiter oder als eigener Verantwortlicher einzuordnen ist, richtet sich nach seiner tatsächlichen Rolle bei der Festlegung von Zweck und Mitteln der Datenverarbeitung im Sinne von Art. 4 Nr. 7 und 8 DSGVO. Massgeblich ist nicht seine vertragliche Bezeichnung, sondern seine Beteiligung an der konkreten Ausgestaltung der Datenverarbeitung.

Ein KI-Anbieter ist als Auftragsverarbeiter im Sinne von Art. 28 DSGVO einzuordnen, wenn er personenbezogene Daten ausschliesslich im Auftrag und nach dokumentierten Weisungen des Kunden verarbeitet und dabei keine eigenen Zwecke verfolgt. Diesfalls ist ein Auftragsverarbeitungsvertrag abzuschliessen. Die Anwendbarkeit von Art. 28 DSGVO setzt insbesondere voraus, dass die Daten nicht für eigene Trainingszwecke, Produktverbesserungen oder sonstige eigenständige Analysen genutzt werden.

Verfolgt der Anbieter solche eigenen Zwecke – etwa indem eingegebene Daten zur Weiterentwicklung des Modells verwendet, mit anderen Datenquellen zusammengeführt oder eigenständig ausgewertet werden –, liegt regelmässig eine eigene oder gemeinsame Verantwortlichkeit im Sinne von Art. 24 oder 26 DSGVO vor. Gerade bei generativen KI-Diensten ist deshalb zu prüfen, ob eine rein weisungsgebundene Verarbeitung tatsächlich gegeben ist oder ob der Anbieter über einen eigenständigen Entscheidungsspielraum bzw. über eigene Nutzungsmöglichkeiten der Daten verfügt.

Organisationen, die ein KI-Tool einsetzen möchten, sind daher gehalten, die konkreten Datenflüsse, die technischen Rahmenbedingungen sowie die vertraglichen Regelungen sorgfältig zu analysieren. Entscheidend für die Beurteilung der Rolle des Anbieters ist stets seine tatsächliche Kontrolle über Zweck und Mittel der Datenverarbeitung.

Gültigkeitsdauer einer Einwilligung

Nach der DSGVO und dem DSG gibt es keine feste gesetzliche Frist, nach der eine einmal erteilte Einwilligung automatisch «abläuft». Stattdessen muss jede Einwilligung im Kontext des konkreten Verarbeitungszwecks und der Verarbeitungstätigkeit bewertet werden. Massgeblich ist, dass personenbezogene Daten und die zugehörigen Einwilligungsnachweise nur so lange gespeichert werden dürfen, wie sie für den ursprünglichen Verarbeitungszweck erforderlich sind und der Zweck weiterhin besteht bzw. auch die betroffenen Personen darauf vertrauen dürfen. Somit muss die Einwilligung regelmässig überprüft werden, um sicherzustellen, dass sie weiterhin den Anforderungen der DSGVO entspricht. Wenn sich die Verarbeitung ändert oder erweitert, ist grundsätzlich eine neue, aktualisierte Einwilligung einzuholen.

Ausserdem haben betroffene Personen zu jedem Zeitpunkt das Recht, ihre Einwilligung zu widerrufen. Dies ist jederzeit möglich und muss so einfach sein wie die Erteilung der Einwilligung selbst. Ein solcher Widerruf wirkt jeweils für die Zukunft und lässt die vor dem Widerruf vorgenommene Datenverarbeitung unberührt. Die bisherige Datenverarbeitung bleibt also auch im Falle eines Widerrufs rechtmässig.

Kurz gesagt: Eine Einwilligung «verfällt» nicht automatisch nach einer bestimmten Zeit, sie sollte aber nur so lange aufbewahrt und genutzt werden, wie sie tatsächlich für die legitimen Zwecke erforderlich

und aktuell ist, und deshalb regelmässig auf ihre Fortgeltung geprüft werden.

2.5 Auswahl konkreter technischer Fragen

Unter den zahlreichen Anfragen zu technischen Themen wurden im Berichtsjahr die folgenden beiden am häufigsten gestellt:

DSGVO-Konformität bestimmter Softwarelösungen oder Cloud-Dienste

Die DSS erhielt in diesem Berichtsjahr mehrfach Anfragen zur DSGVO-Konformität bestimmter Softwarelösungen oder Cloud-Dienste. Die Anfragen wurden häufig allgemein gestellt, ohne spezifische Details wie den geplanten Einsatzzweck oder die konkret verarbeiteten Daten anzugeben. Die DSGVO verlangt allerdings eine eingehende Analyse jedes Einzelfalls einer Verarbeitung personenbezogener Daten. Daher ist eine pauschale datenschutzrechtliche Beurteilung einer Software oder eines Online-Dienstes ohne Kenntnis der spezifischen Details einer geplanten Datenverarbeitung in der Regel nicht möglich. Am Beispiel eines Cloud-Dienstes ist unter anderem zunächst zu prüfen, wie schutzwürdig die verarbeiteten – in der Cloud zu speichernden – Daten sind und welche möglichen Folgen sich für die Betroffenen bei Verlust, Veränderung oder Offenlegung ergeben (Art. 32 DSGVO). Anschliessend ist zu prüfen, ob der jeweilige Cloud-Dienst das zuvor ermittelte erforderliche Schutzniveau erreichen kann. (Schutz-)Massnahmen in der Cloud sind unter anderem Verschlüsselungsmechanismen und Regelungen zu Zugriffsrechten. Unter bestimmten Voraussetzungen ist die vorgenannte Prüfung in Form einer sogenannten Datenschutz-Folgenabschätzung (DSFA) durchzuführen (Art. 35 DSGVO). Im Zusammenhang mit Cloud-Diensten, bei denen die in der Cloud gespeicherten Daten in einen Drittstaat ausserhalb der EU/EWR-Raumes übermittelt werden, ist zudem zu prüfen, ob dieser ein gleichwertiges Schutzniveau für die Daten bietet. Zudem werden Anbieter von Cloud-Diensten häufig als Auftragsverarbeiter gemäss Art. 28 DSGVO qualifiziert, weshalb das Vorliegen eines rechtskonformen Auftragsverarbeitungsvertrages zu prüfen ist. Zusammenfassend kann festgehalten werden, dass der Einsatz einer bestimmten Softwarelösung oder eines Cloud-Dienstes nicht grundsätzlich unzulässig oder zulässig bzw. mit dem Datenschutz unvereinbar oder vereinbar ist. Vielmehr kommt es auf den konkreten Einzelfall und insbesondere auch auf die verarbeiteten personenbezogenen Daten an. Diese Prüfung hat jedoch durch den Verantwortlichen zu erfolgen und nicht durch die DSS.

DSGVO-Konformität der Nutzung öffentlich zugänglicher, Cloud-basierter, generativer KI-Systeme

Im Berichtsjahr erhielt die DSS zahlreiche Anfragen zur datenschutzkonformen Nutzung öffentlich zugänglicher, Cloud-basierter, generativer KI-Systeme. Im Rahmen der Beantwortung dieser Anfragen hielt die DSS stets fest, dass aus verschiedenen Gründen – darunter etwa die äusserst zahlreichen Nutzungsbedingungen, Lizenzmodelle etc., die mitunter auch einem ständigen Wandel durch die Anbieter unterliegen – grundsätzlich keine pauschalen Produkt- oder Versionsbeurteilungen von KI-Systemen durch die DSS vorgenommen werden können. Zudem hängt die datenschutzrechtliche Beurteilung unter anderem wesentlich von der konkreten Konfiguration beim Nutzer sowie von den tatsächlichen Verarbeitungsvorgängen des jeweiligen Systems ab. Generell betonte die DSS, dass vor jeder Nutzung von KI-Systemen mit personenbezogenen Daten insbesondere Fragen zur Rolle des Anbieters, zur Datenverwendung, Rechtsgrundlage, Datensicherheit und zu internationalen Übermittlungen zu klären sind.

Bei vielen grossen, öffentlich zugänglichen, kommerziellen Online-Plattformen und Cloud-Systemen mit KI bestehen derzeit Unsicherheiten hinsichtlich der genauen Rolle der Anbieter, weil die Datenweiterverwendung durch diese häufig intransparent ist. Daher kann derzeit davon ausgegangen werden, dass die Anbieter häufig selbst Verantwortliche sind und eine eigene Rechtsgrundlage für diese Weiterverarbeitung bräuchten (sowohl eine gültige Einwilligung einzuholen als auch ein effektives Widerspruchs- und Widerrufsrecht zu gewähren, scheint aber schwierig zu sein). Einige Anbieter nutzen zudem Server in Drittstaaten, für welche die datenschutzrechtlichen Garantien für die Datenübermittlung geklärt werden müssen. Herausforderungen in Bezug auf Datensicherheit, -richtigkeit und die Umsetzung der Betroffenenrechte treten insbesondere bei sogenannten Large Language Models (LLMs) häufig auf. Dies liegt daran, dass die Anbieter oftmals nicht transparent kommunizieren, ob und wie sie die von den Nutzenden eingegebenen Daten speichern und/oder weiterverwenden – und diese wieder irgendwo (womöglich falsch) ausgeben, selbst wenn die Verwendung zu Trainingszwecken ausgeschlossen wurde.

Vor diesem Hintergrund hielt die DSS fest, dass aus Sicht des Datenschutzes heute (noch) kein vollständig datenschutzkonformer, risikofreier Einsatz solcher Systeme unter Verwendung von personenbezogenen Daten möglich ist. In diesem Zusammenhang weist die DSS jedoch darauf hin, dass die europäischen Datenschutzbehörden derzeit verschiedene Systeme und Techno-

logien untersuchen. Sobald sich hierfür gesicherte Erkenntnisse ergeben, wird die DSS darüber informieren.

2.6 Auswahl wichtiger EuGH-Entscheidungen 2025

Nachdem die Entscheidungen des EuGH für die Beurteilung der Zulässigkeit von Datenverarbeitungen durch die DSS eine zunehmend gewichtige Rolle spielen und von ihr auch regelmässig in die eigenen Entscheidungen einfliessen, wird nachfolgend auf die aus Sicht der DSS bedeutendsten Entscheidungen des EuGH im Berichtsjahr hingewiesen. Zusätzlich erfolgt eine kurze Bewertung, welchen Einfluss diese Entscheidungen auf die Beratung und Aufsicht durch die DSS haben.

EuGH-Urteil vom 9. Januar 2025, C-416/23: Kriterien zur Beurteilung von «exzessiven» Anfragen an Aufsichtsbehörden

Der EuGH hat entschieden, dass Anfragen an eine Aufsichtsbehörde nicht allein aufgrund ihrer Zahl während eines bestimmten Zeitraums als «exzessiv» im Sinne von Art. 57 Abs. 4 DSGVO eingestuft werden können, da die Bestimmung voraussetzt, dass die Aufsichtsbehörde das Vorliegen einer Missbrauchsabsicht der anfragenden Person nachweist. Die betroffene Person hatte bei der Datenschutzaufsichtsbehörde innerhalb eines Zeitraums von ca. 20 Monaten 77 ähnliche Beschwerden gegen verschiedene Verantwortliche eingebracht.

Eine Aufsichtsbehörde kann bei exzessiven Anfragen wählen, ob sie eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangt oder sich weigert, aufgrund der Anfrage tätig zu werden, wobei sie alle relevanten Umstände berücksichtigen und sich vergewissern muss, dass die gewählte Option geeignet, erforderlich und verhältnismässig ist. Sie muss dies in einer mit Gründen versehenen Entscheidung darlegen. Zudem hat der EuGH klargestellt, dass der in Art. 57 Abs. 4 DSGVO enthaltene Begriff «Anfrage» Beschwerden nach Art. 57 Abs. 1 Bst. f und Art. 77 Abs. 1 DSGVO umfasst.

Die DSS war bislang in ihrer Praxis nie in der Situation, von exzessiven Beschwerden im Sinne eines missbräuchlichen Vorgehens ausgehen zu müssen. Zwar gibt es Einzelfälle, in denen Personen wiederholt oder auch regelmässig Beschwerden einbringen. Diese werden jedoch jeweils formell und materiell geprüft und nach Massgabe der nationalen Vorschriften, insbesondere des Landesverwaltungsgesetzes, behandelt. Eine pauschale Einstufung als exzessiv allein aufgrund der Anzahl der Eingaben erfolgte durch die DSS bislang nicht.

Demgegenüber wird das Argument der Exzessivität regelmässig von Beschwerdegegnern vorgebracht. Die DSS hat insoweit stets einen strengen Prüfungsmassstab angelegt. Eine Einschränkung des Tätigwerdens gestützt auf Art. 57 Abs. 4 DSGVO kam bisher nicht zur Anwendung und ging noch nie zu Lasten einer beschwerdeführenden Person.

Das Urteil bestätigt somit im Wesentlichen die bisherige Praxis der DSS, wonach das Beschwerderecht als zentrales Instrument der Rechtsdurchsetzung nur in klaren Ausnahmefällen und unter strikter Wahrung des Verhältnismässigkeitsprinzips eingeschränkt werden darf.

EuGH-Urteil vom 13. Februar 2025, C-383/23: Geldbussen und der Begriff «Unternehmen»

Gemäss EuGH entspricht der Begriff «Unternehmen» aus Art. 83 Abs. 4 bis 6 DSGVO dem Begriff «Unternehmen» im Sinne der Art. 101 und 102 AEUV. Unter einem Unternehmen im Sinne des Art. 83 Abs. 4 bis 6 DSGVO ist demnach eine wirtschaftliche Einheit zu verstehen, auch wenn diese in rechtlicher Hinsicht aus mehreren natürlichen oder juristischen Personen besteht. Das bedeutet, dass der Höchstbetrag einer Geldbusse, die gegen einen Verantwortlichen wegen eines Verstosses gegen die DSGVO verhängt wird, auf der Grundlage eines Prozentsatzes des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres des Unternehmens bestimmt wird.

Der Begriff «Unternehmen» ist auch zu berücksichtigen, um die tatsächliche oder materielle Leistungsfähigkeit des Adressaten der Geldbusse zu beurteilen und so zu überprüfen, ob die Geldbusse sowohl wirksam und verhältnismässig als auch abschreckend ist. Diverse Unternehmen hatten in der Vergangenheit mit getrennten Einheiten (Tochterunternehmen etc.) argumentiert, um die Geldbusse niedrig zu halten.

Diese Entscheidung des EuGH wirkt weit über den Anwendungsbereich der DSGVO hinaus. Auch die KI-Verordnung, der Digital Markets Act und der Digital Services Act enthalten ähnliche Bussgeldbestimmungen, für die dieses Urteil massgebend sein wird.

Auch wenn in Liechtenstein bislang Geldbussen nur gegen Unternehmen ausgesprochen wurden, bei denen kein weltweiter Konzernumsatz zu be-

rücksichtigen war, stellt das Urteil eine klare Bestätigung der in der DSGVO vorgesehenen Systematik der Bussgeldbemessung dar. Es schiebt Umgehungsversuchen, etwa durch die Aufspaltung wirtschaftlicher Einheiten in mehrere, formell getrennte Gesellschaften zur Reduktion des zur Berechnung relevanten Umsatzes, einen deutlichen Riegel vor.
Die DSS weist allerdings darauf hin, dass auch rein national tätige Unternehmen in Einzelfällen versuchen, ihre massgeblichen Umsatzzahlen durch unterschiedliche gesellschaftsrechtliche oder buchhalterische Gestaltungen zu reduzieren, um die Bemessungsgrundlage einer allfälligen Geldbusse zu beeinflussen. Ein entsprechender Fall ist derzeit bei der zuständigen Beschwerdekommission für Verwaltungsangelegenheiten (VBK) hängig. Die DSS erhofft sich von dieser Entscheidung zusätzliche Klarheit hinsichtlich der Offenlegung und Beurteilung relevanter Umsatzzahlen im Bussgeldverfahren.

EuGH-Urteil vom 27. Februar 2025, C-203/22: Auskunftsrecht bei automatisierten Entscheidungen und bei Geschäftsgeheimnissen

Der EuGH entschied, dass Art. 15 Abs. 1 Bst. h DSGVO dahingehend auszulegen ist, dass Unternehmen bei automatisierten Entscheidungsfindungen (einschliesslich Profiling) im Sinne von Art. 22 Abs. 1 DSGVO der betroffenen Person detailliert über die eingesetzten Verfahren Auskunft geben müssen.

Eine Wirtschafts-Auskunftei hatte die Offenlegung ihrer Scoring-Logik unter Berufung auf das Geschäftsgeheimnis verweigert. Der EuGH hat jedoch entschieden, dass Unternehmen verpflichtet sind, den Betroffenen zumindest die Verfahren und Grundsätze bei automatisierten Entscheidungen in präziser, transparenter, verständlicher und leicht zugänglicher Form zu erläutern. Betroffene müssen die Informationen in vollem Umfang verstehen können, weshalb die mitgeteilten Informationen allenfalls zu kontextualisieren sind. Darüber hinaus sind Unternehmen jedenfalls verpflichtet, Geschäftsgeheimnisse im Sinne von Art. 2 Nr. 1 der Richtlinie (EU) 2016 / 943 gegenüber der zuständigen Datenschutzaufsichtsbehörde oder einem zuständigen Gericht offenzulegen. Die Datenschutzaufsichtsbehörde bzw. das Gericht hat in der Folge abzuwägen, ob und inwieweit Geschäftsgeheimnisse für die betroffene Person relevant sind und offengelegt werden müssen.

Im konkreten Fall ging es darum, dass der betroffenen Person aufgrund eines KI-gestützten Bonitäts-Scorings mangels Kreditwürdigkeit ein Vertragsabschluss verweigert worden war.

Die DSS hatte bislang keine Beschwerdefälle zu automatisierter Entscheidungsfindung im engeren Sinne von Art. 22 DSGVO zu beurteilen. Zunehmend ist jedoch festzustellen, dass Beschwerdegegner im Rahmen von Auskunftsersuchen nach Art. 15 DSGVO geltend machen, bestimmte Informationen könnten wegen angeblicher Geschäftsgeheimnisse nicht offengelegt werden – ohne diese näher zu spezifizieren.
In sämtlichen bisher geprüften Fällen stellte sich heraus, dass die Voraussetzungen eines Geschäftsgeheimnisses nicht erfüllt waren. Der unionsrechtliche Begriff des Geschäftsgeheimnisses geht nämlich über das umgangssprachliche Verständnis hinaus und richtet sich nach der Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung. Geschützt sind demnach nur solche Informationen, die geheim sind, wirtschaftlichen Wert gerade aufgrund ihrer Geheimhaltung besitzen und Gegenstand angemessener Geheimhaltungsmassnahmen sind. Eine bloss interne oder betriebsinterne Information genügt hierfür nicht.
Das Urteil bestätigt damit die bisherige Praxis der DSS, wonach eine Berufung auf Geschäftsgeheimnisse nicht schematisch akzeptiert wird, sondern einer substanziellen Begründung bedarf. Bevor man sich auf das Geschäftsgeheimnis beruft, um eine Auskunft zu verweigern, sollte somit immer geprüft werden, ob wirklich alle drei Kriterien der erwähnten Richtlinie erfüllt sind; insbesondere, ob die geheime Information nicht nur geheim ist, sondern auch kommerziellen Wert hat.

EuGH-Urteil vom 4. September 2025, C-413/23: Pseudonymisierung – Relativität des Personenbezugs

Der EuGH hat entschieden, dass pseudonymisierte Stellungnahmen, die persönliche Meinungen enthalten, nicht in jedem Fall personenbezogene Daten darstellen müssen. So ist bei einer Weitergabe der Daten an Dritte entscheidend, ob der Empfänger die betroffene Person noch identifizieren kann oder ob die Pseudonymisierung eine Identifizierbarkeit wirksam verhindert, sodass die Daten für den Empfänger faktisch

anonymisiert sind. Demnach sind pseudonymisierte Daten nicht in jedem Fall und für jede Person als personenbezogene Daten zu betrachten, sondern es hat eine relative Beurteilung zu erfolgen. Ob eine Identifizierbarkeit (zumindest als theoretische Möglichkeit) durch den Empfänger besteht, hängt massgeblich von den konkreten Umständen im Einzelfall ab. Stehen dem Empfänger keine Mittel (z.B. ergänzende Informationen oder technische «Schlüssel», die eine erneute Herstellung des Personenbezugs ermöglichen) zur Re-Identifizierung der natürlichen Person zur Verfügung oder ist eine Zuordnung gesetzlich verboten oder praktisch nicht durchführbar, liegen für den Empfänger keine personenbezogenen Daten vor. Die Vorgaben des Datenschutzrechts finden somit für den Empfänger keine Anwendung. Für den ursprünglich Verantwortlichen stellen die Daten jedoch in jedem Fall personenbezogene Daten dar, weswegen er den datenschutzrechtlichen Pflichten nach DSGVO vollumfänglich unterliegt.

Die DSS folgt diesem relativen Verständnis bereits seit 2019. In einem damaligen Fall übermittelte ein Verantwortlicher in Liechtenstein pseudonymisierte Daten an einen Auftragsverarbeiter in der Schweiz, der daraus eine anonymisierte Statistik erstellte. Aus Sicht des Auftragsverarbeiters waren die Daten faktisch anonym, da er über keinerlei rechtlich zulässige Mittel verfügte, Zugang zum Identifizierungsschlüssel oder zu anderen für eine Re-Identifizierung erforderlichen Informationen zu erhalten. Die DSS gelangte daher zur Auffassung, dass für den Auftragsverarbeiter im konkreten Fall keine personenbezogenen Daten vorlagen.

Zu einem vergleichbaren Ergebnis kam die DSS kürzlich in einem Beschwerdefall, in dem ein Verantwortlicher versehentlich eine E-Mail an zahlreiche unbefugte Empfänger versandt hatte, worin auch die E-Mail-Adresse des Beschwerdeführers ersichtlich war. Die E-Mail-Adresse des Beschwerdeführers enthielt jedoch nicht dessen Namen, sondern war pseudonymisiert. Da die übrigen Empfänger über keinerlei rechtliche oder faktische Mittel verfügten, die Identität des Beschwerdeführers zu ermitteln, war die E-Mail-Adresse aus ihrer Perspektive anonymisiert und stellte kein personenbezogenes Datum des Beschwerdeführers dar. Es lag somit keine unbefugte Offenlegung personenbezogener Daten vor und die DSS wies die Beschwerde zurück. Auch hier wurde die Beurteilung von der DSS für den konkreten Fall und akteursbezogen vorgenommen.

Die DSS weist jedoch darauf hin, dass dieser relative Ansatz zwar in klar gelagerten, technisch überschaubaren Konstellationen praktikabel und sachgerecht ist, in komplexeren Sachverhalten jedoch neue Abgrenzungsfragen aufwerfen kann. Insbesondere bei umfangreichen und komplexen Datenverarbeitungen oder bei mehreren beteiligten Akteuren kann die Bewertung der tatsächlichen Identifizierungsmöglichkeiten anspruchsvoll sein. Das Urteil bestätigt somit die bisherige Praxis der DSS, macht aber zugleich deutlich, dass eine sorgfältige, kontextbezogene Analyse unerlässlich bleibt.

«Die detaillierten Stellungnahmen ermöglichten es, datenschutzrelevante Aspekte zu identifizieren, zu analysieren und gegebenenfalls Anpassungen vorzuschlagen, um sicherzustellen, dass die Gesetzgebung den aktuellen Datenschutzstandards gerecht wird.»

3. Stellungnahmen zu Vorlagen und Erlassen

Im Berichtsjahr war die DSS wieder stärker als in den Vorjahren bereits in den eigentlichen Gesetzgebungsprozess integriert worden und konnte die zuständigen Amtsstellen schon bei der Ausarbeitung der Gesetzesvorlagen umfassend beraten. So konnte unter anderem bei der nationalen Umsetzung der KI-Verordnung, des Data Governance Acts oder auch bei der Revision des FIU-Gesetzes substanziell beratend mitgewirkt werden. Formell prüfte die DSS im Verlauf des Berichtsjahres insgesamt 26 ausgearbeitete Gesetzesvorlagen und Erlasse. Bei 12 dieser Vorlagen stellte die DSS fest, dass entweder keine datenschutzrechtlichen Aspekte betroffen waren oder dass die entsprechenden Elemente in Übereinstimmung mit den geltenden Datenschutzbestimmungen umgesetzt wurden. Bei der Gesetzesvorlage zur Abänderung des Datenschutzgesetzes verzichtete die DSS auf eine Stellungnahme, da sie bereits in der vorbereitenden Arbeitsgruppe aktiv mitgewirkt hatte. In Bezug auf 13 Vorlagen und Erlasse erstellte die DSS ausführliche inhaltliche Stellungnahmen. Diese detaillierten Stellungnahmen ermöglichten es, datenschutzrelevante Aspekte zu identifizieren, zu analysieren und gegebenenfalls Anpassungen vorzuschlagen, um sicherzustellen, dass die Gesetzgebung den aktuellen Datenschutzstandards gerecht wird. Die umfangreichsten Stellungnahmen der DSS werden nachfolgend kurz beschrieben.

In Bezug auf den **Vernehmlassungsbericht (VNB) der Regierung betreffend die Abänderung des Strafgesetzbuches, der Strafprozessordnung, des Strafvollzugsgesetzes, des Gesetzes über das Strafregister und die Tilgung gerichtlicher Verurteilungen, des Staatsanwaltschaftsgesetzes sowie des Jugendgerichtsgesetzes** traf die DSS folgende Feststellungen:

Die DSS anerkennt, dass im VNB zentrale Aspekte des Grundrechtsschutzes und des Datenschutzes bei der Einführung der optischen und akustischen Überwachung von Personen berücksichtigt wurden. Gleichwohl sieht sie in mehreren Punkten Klärungs- und Präzisierungsbedarf. Grundsätzlich stellt die geplante Überwachung einen erheblichen Eingriff in das Recht auf Privatsphäre dar, der zwar unter bestimmten Voraussetzungen gerechtfertigt sein kann, jedoch keinesfalls den Kernbereich privater Lebensgestaltung berühren darf. Die DSS fragt daher, wie im Rahmen der Anordnung sichergestellt werde, dass dieser Kernbereich nicht tangiert wird, und wie vorzugehen sei, falls dennoch kernbereichsrelevante Daten erhoben werden – insbesondere, wie deren Nichtverwendung bzw. Löschung garantiert wird.

Weiter weist die DSS auf terminologische Unklarheiten in § 104e StPO hin, da dort teils von «Beschuldigten» und teils von «verdächtigten Personen» die Rede ist. Es stellt sich die Frage, ob diese Differenzierung beabsichtigt ist oder ob aus Gründen der Systematik und Rechtsklarheit ein einheitlicher Begriff verwendet werden sollte. In Bezug auf § 104f StPO kritisiert die DSS, dass zwar gesetzlich vorgesehen ist, die Überwachungsmassnahme zu beenden, sobald deren Voraussetzungen wegfallen, dass jedoch aus dem Gesetzestext selbst nicht hervorgeht, wer diese Beurteilung trifft. Die entsprechenden Zuständigkeitsregelungen finden sich lediglich in den Erläuterungen. Aus Gründen der Rechtssicherheit und Transparenz regt die DSS an, diese Rollenverteilung ausdrücklich im Gesetz zu verankern.

Hinsichtlich § 104g StPO wird darauf hingewiesen, dass der Untersuchungsrichter im Beschluss den Beginn und das Ende der Überwachung festlegen muss und damit über deren Dauer entscheidet. Die DSS empfiehlt hier die Einführung einer gesetzlichen Höchstdauer, um eine periodische richterliche Überprüfung sicherzustellen und gegebenenfalls eine Verlängerung nur bei fortbestehender Rechtfertigung zu ermöglichen. Zudem sollte der Katalog der Beschlussinhalte um eine ausdrückliche Begründung der Erforderlichkeit und Verhältnismässigkeit der Massnahme ergänzt werden. Aus datenschutzrechtlicher Sicht ist es ferner angezeigt, auch den konkreten Zweck beziehungsweise den zugrunde liegenden Tatvorwurf im Beschluss zu benennen.

Bezüglich § 104h Abs. 1 StPO bemängelt die DSS eine unklare Formulierung und empfiehlt – in Anlehnung an die österreichische Vorlage – eine strukturierte Aufzählung der einzelnen Varianten zur Verbesserung der Verständlichkeit. Zu § 104h Abs. 2 StPO stellt sie eine Diskrepanz zwischen Gesetzestext und Erläuterungen fest: Während der Gesetzestext die Zulässigkeit der Verwendung von Zufallsfunden einschränkt, lassen die Erläuterungen eine weitergehende Verwendung auch bei Straftaten mit geringerer Strafdrohung zu. Die dort genannten Strafrahmen von einem Jahr beziehungsweise sechs Monaten Freiheitsstrafe stimmen nach Ansicht der DSS nicht mit den im Gesetz formulierten Voraussetzungen überein.

Abschliessend kritisiert die DSS, dass die vorgesehenen Bestimmungen keine expliziten Regelungen

zur Löschung der durch die Überwachung gewonnenen personenbezogenen Daten enthalten. Zwar verpflichtet § 104g Abs. 2 StPO den Untersuchungsrichter, die Ergebnisse zu prüfen und nur verfahrensrelevante Teile zu den Akten zu nehmen, doch bleibt unklar, was mit den übrigen Daten geschieht. Die DSS empfiehlt daher, ergänzend klare Löschregelungen vorzusehen und sich dabei an § 145 Abs. 1–3 der österreichischen Strafprozessordnung zu orientieren.

In Bezug auf den **Vernehmlassungsbericht (VNB) der Regierung betreffend die Abänderung des Polizeigesetzes** nahm die DSS umfassend Stellung und wies auf folgende kritische Punkte hin:

Ausgangspunkt der Revision ist gemäss Zusammenfassung die Umsetzung der sogenannten Istanbul-Konvention zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt. Die DSS kritisiert jedoch, dass in der Zusammenfassung lediglich beiläufig auf weitere, in ihrer Tragweite erhebliche Änderungen hingewiesen wird. Insbesondere betreffen diese die Einführung einer automatisierten Fahrzeugfahndung mittels Kennzeichenerfassung (ANPR) sowie neue präventive Befugnisse der Landespolizei zur Verhinderung terroristischer und sonstiger schwerer Straftaten. Diese Massnahmen sind aus Sicht der DSS mit erheblichen Grundrechtseingriffen verbunden und sollten aus Gründen der rechtsstaatlichen Transparenz in der Zusammenfassung gleichwertig dargestellt werden.

Zur automatisierten Fahrzeugfahndung hält die DSS fest, dass Nummernschilder personenbezogene Daten darstellen, da sie (auch) einer bestimmten natürlichen Person zugeordnet werden können. Bereits die automatisierte Erfassung und der Abgleich – unabhängig davon, ob ein Treffer vorliegt – greifen in das Recht auf informationelle Selbstbestimmung ein. Eine solche Massnahme bedarf daher einer klaren, präzisen gesetzlichen Grundlage mit eindeutig definierten Voraussetzungen, strenger Zweckbindung sowie wirksamen Kontroll- und Löschregelungen. In Bezug auf Art. 24d^{bis} Abs. 1 PolG bemängelt die DSS, dass zwar verschiedene Zwecke aufgelistet werden, jedoch insbesondere im Bereich des Staatsschutzes weitergehende Konkretisierungen erforderlich sind, damit polizeiliches Handeln vorhersehbar und kontrollierbar bleibt. Auch zu den übrigen Tatbeständen sind detailliertere Erläuterungen im Bericht wünschenswert.

Besonders kritisch beurteilt die DSS Art. 24d^{bis} Abs. 3 PolG, wonach Nummernschild, Zeitpunkt (und mutmasslich Fahrtrichtung) für bis zu 30 Tage gespeichert werden dürfen. Obwohl keine Bilddaten gespeichert werden sollen, stellt diese Regelung eine Art anlasslose Vorratsdatenspeicherung dar. In einem Rechtsstaat darf staatliche Überwachung jedoch grundsätzlich nicht ohne konkreten Anlass erfolgen. Für den unmittelbaren Abgleich mit polizeilichen Systemen ist eine darüberhinausgehende Speicherung nicht erforderlich. Die vorgesehene Aufbewahrung geht daher über den ursprünglichen Zweck hinaus und ist unverhältnismässig. Die DSS empfiehlt, Abs. 3 zu streichen und klarzustellen, dass bei Nichttreffern keinerlei Daten gespeichert werden dürfen. Offen bleibt zudem, wie mit sogenannten «unechten Treffern» (false positives) umzugehen ist. Weder Gesetz noch Erläuterungen enthalten hierzu ausreichende Vorgaben. Die DSS verlangt eine präzise Regelung, um Fehlzuordnungen datenschutzkonform zu behandeln.

Auch Art. 24d^{bis} Abs. 4 PolG ist zu konkretisieren: Der Polizeichef muss bei der Anordnung der Massnahme bestimmte Voraussetzungen – etwa eine Lageanalyse – berücksichtigen; flächendeckende oder zeitlich übermässige Einsätze sind auszuschliessen. Kontrollen dürfen nur punktuell, örtlich und zeitlich begrenzt erfolgen. Da zudem ein Abgleich mit internationalen Datenbanken wie dem Schengener Informationssystem (SIS) und Interpol vorgesehen ist, sind die entsprechenden unionsrechtlichen Voraussetzungen einzuhalten. Art. 24d^{bis} Abs. 6 PolG schliesslich bedarf einer Präzisierung hinsichtlich der Protokollierungspflichten, da eine effektive datenschutzrechtliche Kontrolle nur auf Grundlage aussagekräftiger Dokumentation möglich ist. Darüber hinaus weist die DSS auf die einschlägigen Informationspflichten nach DSG und DSGVO hin, da die Massnahmen teilweise in deren Anwendungsbereich fallen.

In Bezug auf Art. 24g^{bis} Abs. 2 PolG, der die Übermittlung von Dokumentationen bei Betretungsverboten an eine Beratungsstelle vorsieht, regt die DSS an, eine Datenweitergabe erst dann zuzulassen, wenn die Notwendigkeit einer Gewaltpräventionsberatung rechtlich gesichert ist. Da ein Betretungsverbot binnen 72 Stunden überprüft und aufgehoben werden kann, wäre eine sofortige Datenübermittlung unter Umständen unverhältnismässig.

Besonders kritisch beurteilt die DSS die Einführung des neuen Art. 26a PolG, welcher der Landespolizei weitreichende präventive Massnahmen zur Verhinderung terroristischer und sonstiger schwerer Straftaten einräumt. Dabei handelt es sich um tiefgreifende Eingriffe in Grundrechte, insbesondere in die Bewegungsfreiheit und das soziale Leben der betroffenen Personen, und zwar gestützt auf einen blossen Verdacht ohne vorgängiges Gerichtsurteil. Eine derart intensive Einschränkung verlangt eine besonders präzise gesetzliche Grundlage sowie eine umfassende Verhältnismässigkeitsprüfung im Gesetzgebungsver-

fahren. Die DSS wirft zudem spezifische Fragen auf: So ist unklar, wie sich die vorgesehene Gesprächspflicht gegenüber der Polizei zu einem allfälligen Zeugnisverweigerungsrecht verhält. Ebenso bleibt offen, ob eine Person, die zwar physisch an einem Gespräch teilnimmt, jedoch schweigt, ihre Pflicht erfüllt oder mit einer Busse rechnen muss. Problematisch erscheint auch die Regelung zur Befristung der Massnahmen auf sechs Monate mit einmaliger Verlängerungsmöglichkeit. In der vorgesehenen Ausgestaltung können die Massnahmen faktisch unbeschränkt verlängert werden, indem sie jeweils kurzzeitig unterbrochen und erneut angeordnet werden. Dies wäre mit den verfassungsrechtlichen Anforderungen nur schwer vereinbar.

Hinsichtlich der Videoüberwachung (Art. 34 Abs. 3 und 4 PolG) weist die DSS darauf hin, dass durch die Ausdehnung auf die Suche nach Vermissten der Anwendungsbereich der einschlägigen datenschutzrechtlichen Vorschriften erweitert wird. Die daraus folgenden Informationspflichten sind entsprechend zu berücksichtigen.

Abschliessend bemängelt die DSS, dass im Gesetzgebungsverfahren keine umfassende, dokumentierte Verhältnismässigkeitsprüfung vorgenommen wurde. Gerade angesichts der erheblichen Grundrechtseingriffe – insbesondere durch Art. 26a PolG – ist eine vertiefte Grundrechtsprüfung unerlässlich. Der Gesetzgeber ist verpflichtet, neben einer klaren gesetzlichen Grundlage stets auch dem Grundsatz der Verhältnismässigkeit Rechnung zu tragen. Eine solche Prüfung ist hier nicht nur rechtsstaatlich geboten, sondern angesichts der Tragweite der vorgesehenen Massnahmen zwingend erforderlich.

In Bezug auf den **Vernehmlassungsbericht (VNB) der Regierung betreffend die Abänderung des Wertpapierdienstleistungsgesetzes, des Vermögensverwaltungsgesetzes, des Handelsplatz- und Börsegesetzes, EWR-Wertpapierprospekt-Durchführungsgesetzes, des EWR-Marktmissbrauchsverordnungs-Durchführungsgesetzes und weiterer Gesetze** empfiehlt die DSS vor allem die geplante Anpassung von Art. 30 Wertpapierfirmengesetz zu überdenken.

Gemäss Vernehmlassungsbericht soll Art. 30 Wertpapierfirmengesetz im Wortlaut geändert und mit Art. 42 Vermögensverwaltungsgesetz sowie Art. 15 Bankengesetz harmonisiert werden. Künftig soll ausdrücklich vorgesehen sein, dass Wertpapierfirmen personenbezogene Daten, einschliesslich besonderer Kategorien personenbezogener Daten sowie Daten über strafrechtliche Verurteilungen und Straftaten, verarbeiten dürfen, soweit dies für die Erbringung von Wertpapier- und Nebendienstleistungen oder für Anlagetätigkeiten erforderlich ist. Inhaltlich kritisiert die DSS, dass diese Bestimmungen pauschale gesetzliche Grundlagen für die Datenverarbeitung durch die betroffenen Unternehmen schaffen. Dies widerspricht dem System der DSGVO, welche die zulässigen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten in Art. 6 Abs. 1 abschliessend regelt, für besondere Kategorien personenbezogener Daten in Art. 9 Abs. 2 und für Daten über strafrechtliche Verurteilungen und Straftaten in Art. 10. Nationale Gesetzgeber dürfen nur im Rahmen der in der DSGVO vorgesehenen Öffnungsklauseln ergänzende Regelungen treffen, und auch dies nur unter strengen Voraussetzungen.

Für besondere Kategorien personenbezogener Daten kommt vorliegend allenfalls Art. 9 Abs. 2 Bst. g DSGVO als Rechtsgrundlage in Betracht. Diese Bestimmung erlaubt eine Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses, sofern eine gesetzliche Grundlage besteht, die verhältnismässig ist, den Wesensgehalt des Datenschutzrechts wahrt und angemessene Schutzmassnahmen vorsieht. Bei den vorgesehenen Regelungen fehlt jedoch ein solches erhebliches öffentliches Interesse. Die Datenverarbeitung in den genannten Gesetzen wird zur Erbringung kommerzieller Dienstleistungen erlaubt. Eine rein wirtschaftliche Tätigkeit stellt kein erhebliches öffentliches Interesse im Sinne der DSGVO dar. Die Bestimmungen stehen daher in Widerspruch zu Art. 9 Abs. 2 DSGVO. Zwar benötigen Vermögensverwalter, Banken oder Wertpapierfirmen in Einzelfällen bestimmte sensible Daten, etwa zur Erfüllung gesetzlicher Prüfpflichten. Solche Konstellationen müssen jedoch präzise gesetzlich umschrieben werden und können keinesfalls kommerzielle Dienstleistungen mitumfassen. Die aktuelle Formulierung ist daher zu allgemein und genügt den Anforderungen der DSGVO nicht.

Auch im Hinblick auf Art. 6 DSGVO besteht ein vergleichbares Problem. Art. 6 Abs. 2 DSGVO erlaubt nationale Präzisierungen nur im Zusammenhang mit einer gesetzlichen Verpflichtung (Art. 6 Abs. 1 Bst. c DSGVO) oder der Wahrnehmung einer Aufgabe im öffentlichen Interesse (Art. 6 Abs. 1 Bst. e DSGVO). Die Erbringung kommerzieller Finanzdienstleistungen erfüllt keine dieser Voraussetzungen. Eine generelle gesetzliche Erlaubnis zur Datenverarbeitung für Geschäftszwecke überschreitet daher den zulässigen Rahmen. Falls die Unternehmen Daten zur Erfüllung spezifischer gesetzlicher Pflichten – etwa nach dem Sorgfaltspflichtgesetz – verarbeiten, sind diese Pflichten bereits in den entsprechenden Spezialgesetzen geregelt. Eine zusätzliche, pauschale Ermächtigungs-

norm in den hier betroffenen Gesetzen ist daher nicht erforderlich.

Die DSS weist zudem auf eine inkonsistente Gesetzgebung hin. Entsprechende Datenverarbeitungsbestimmungen finden sich in einzelnen finanzmarktrechtlichen Gesetzen, fehlen jedoch in anderen regulierten Bereichen wie etwa im Treuhänderrecht oder im Versicherungsrecht. Dies führt zu einer Ungleichbehandlung regulierter Unternehmen und steht im Spannungsverhältnis zu datenschutzrechtlichen Grundprinzipien.

Aus diesen Gründen empfiehlt die DSS, vorerst auf die geplante Änderung von Art. 30 Wertpapierfirmengesetz zu verzichten. Unabhängig vom laufenden Vernehmlassungsverfahren regt sie eine vertiefte Prüfung der bestehenden gesetzlichen Bestimmungen im Hinblick auf ihre Vereinbarkeit mit der DSGVO an.

«Sollte auch für das Jahr 2027 keine Erhöhung des Personalbestandes genehmigt werden, sind weitere Priorisierungen unausweichlich.»

4. Interne Organisation

Die DSS ist die nationale Datenschutz-Aufsichtsbehörde im Sinne des Art. 51 DSGVO sowie des Art. 9 DSG. Sie übt ihre Befugnisse in vollständiger Unabhängigkeit aus und untersteht keiner Dienst- oder Fachaufsicht. Die Aufgaben der DSS ergeben sich direkt aus der DSGVO und dem DSG sowie einzelnen Bestimmungen in Spezialgesetzen.

4.1 Personal allgemein

Im Tätigkeitsbericht 2024 hielt die DSS fest, dass sie ihre gesetzlichen Aufgaben trotz hoher Anforderungen mit einem Personalbestand von insgesamt 700 Stellenprozenten erfüllen konnte. Gleichzeitig wies sie darauf hin, dass keine Reserven mehr vorhanden sind und künftig bereits geringfügige Mehrbelastungen nicht mehr aufgefangen werden können. Vor diesem Hintergrund beantragte die DSS die Genehmigung von mindestens einer zusätzlichen Juristenstelle, um die Aufgabenerfüllung nachhaltig sicherzustellen. Dieser Antrag wurde abgelehnt.

Bereits in den vergangenen Jahren war der Aufwand für die Beantwortung der mannigfachen Beratungsanfragen stetig gestiegen und das Volumen von Beschwerden gemäss Art. 77 DSGVO und Meldungen von Datenschutzverletzungen gemäss Art. 33 DSGVO nahm kontinuierlich zu. Die personellen Ressourcen der DSS waren somit schon in den letzten Jahren stark absorbiert in der Verfassung von Antworten und Stellungnahmen auf konkrete Fragen, der technischen Untersuchung und Analyse von Systemen und Meldungen, sowie der Prüfung der eingegangenen Beschwerden und Hinweise und der Führung der entsprechenden Verfahren. Dazu kamen eine immer stärkere Einbindung der DSS in zahlreiche Gesetzgebungsverfahren oder Arbeitsgruppen der LLV aufgrund der voranschreitenden Digitalisierung.

Im Berichtsjahr verschärfte sich dieser Trend nun nochmals deutlich, was eine weitere beträchtliche Erhöhung des Arbeitsvolumens der DSS nach sich zog. Die Komplexität der Beratungsanfragen, doch insbesondere die Zahl der Beschwerden gemäss Art. 77 DSGVO sowie der Meldungen von Datenschutzverletzungen gemäss Art. 33 DSGVO nahm 2025 enorm zu, rund 50 % bei den Beschwerden und rund 35 % bei den Meldungen. Dies scheint nach ähnlichen Aussagen anderer Datenschutz-Aufsichtsbehörden einem europäischen Trend zu entsprechen und es ist keine Veränderung in den kommenden Jahren zu erwarten. Parallel dazu entstanden für die DSS zusätzliche Aufgaben im Zusammenhang mit der Vorbereitung und Umsetzung weiterer EU-Digitalrechtsakte, insbesondere der KI-Verordnung, des Data Act und des Data Governance Act. Auch die Reform des FIU-Gesetzes wurde von der DSS eng begleitet und wird voraussichtlich weitere Kontrollaufgaben nach sich ziehen. Daneben war die DSS im Berichtsjahr in die Arbeitsgruppe der LLV zu M365-Copilot involviert, hat die ZPR-Kommission wieder beratend unterstützt, wurde in die Task Force zur Prüfung von Handlungsbedarf und Massnahmen betreffend Datenschutz im schulischen Umfeld aufgenommen und beteiligte sich im Rahmen der Kompetenzgruppe Digitalisierung bei der Nutzungsregelung von KI in der LLV. All diese Entwicklungen führen mittlerweile zu einer beträchtlichen Überlastung.

Folglich kam es im Berichtsjahr vor allem bei der Beantwortung von Beratungsanfragen bereits zu spürbaren Verzögerungen. Darüber hinaus musste die DSS Priorisierungen vornehmen und einzelne Aufgaben vollständig einstellen. So musste sie bereits die Durchführung von nicht-anlassbezogenen amtswegigen Datenschutzüberprüfungen aussetzen und die Frequenz von Veranstaltungen und Newslettern reduzieren, was nicht nur die Aufsichtstätigkeit einschränkt, sondern auch der bewährten kommunikativen Strategie der DSS schadet. Darüber hinaus stellte sie ihre Mitwirkung im European Fundamental Rights Guidance Board (EFRGB) sowie in der Arbeitsgruppe zum Zusammenspiel von Datenschutz und anderen Rechten und Freiheiten der Global Privacy Assembly (GPA) weitgehend ein und hat bis auf eine Ausnahme keine aktiven Aufgaben oder Rollen im Rahmen des EDSA mehr übernommen. Ebenso wenig wird sie sich 2026 an der koordinierten Aktion der europäischen Datenschutz-Aufsichtsbehörden für ein bestimmtes Datenschutzthema beteiligen. Und künftig wird sie, sollte sich an der Situation nichts ändern, auch LLV-intern ihre Beratungen und Schulungen im Rahmen der LLV-Akademie nicht mehr im gewohnten Umfang anbieten können. Exemplarisch für diese Entwicklung konnte sie für den Fachstab Cyber nur einen statt der gewünschten zwei Vertreter nominieren und musste zudem festhalten, dass keine Kapazitäten für eine aktive Mitarbeit zur Verfügung stehen. Des Weiteren ist aufgrund des Personalmangels für das Jahr 2026 kein «Datenschutz goes Cinema» geplant. Schliesslich musste auch die Entsendung eines Juristen zur Teilnahme an einer Schengen-Evaluation in einem an-

deren Schengen-Staat 2026 mangels personeller Ressourcen abgesagt werden.

Sollte auch für das Jahr 2027 keine Erhöhung des Personalbestandes genehmigt werden, sind weitere Priorisierungen unausweichlich. Da die Beratungstätigkeit im Gegensatz zu den Aufsichtstätigkeiten nicht ausdrücklich gesetzlich vorgeschrieben ist, bleibt sie faktisch als einziger Bereich, in welchem weitere Einschränkungen vorgenommen werden können. Dies führt dazu, dass öffentliche Stellen und Unternehmen künftig deutlich längere Antwortzeiten in Kauf nehmen oder ganz auf eine vorgängige datenschutzrechtliche Beratung verzichten müssen, was das Risiko von Rechtsunsicherheiten und Fehlumsetzungen erhöht.

4.2 Personal Schengen-Evaluation

Die gesetzlichen Grundlagen diverser EU-Informationssysteme im Schengen-Raum sehen vor, dass diese alle vier Jahre einer datenschutzrechtlichen Kontrolle unterzogen werden müssen. Aufgrund der Mitgliedschaft Liechtensteins im Schengen-Raum entsandte die DSS im Berichtsjahr in einem Fall einen Experten zwecks Evaluierung eines anderen Schengen-Staates. Nach regelmässiger jährlicher Teilnahme mindestens eines Mitarbeitenden der DSS an einer solchen Evaluierung in einem anderen Mitgliedstaat muss die DSS 2026 auf eine Entsendung mangels Ressourcen verzichten.

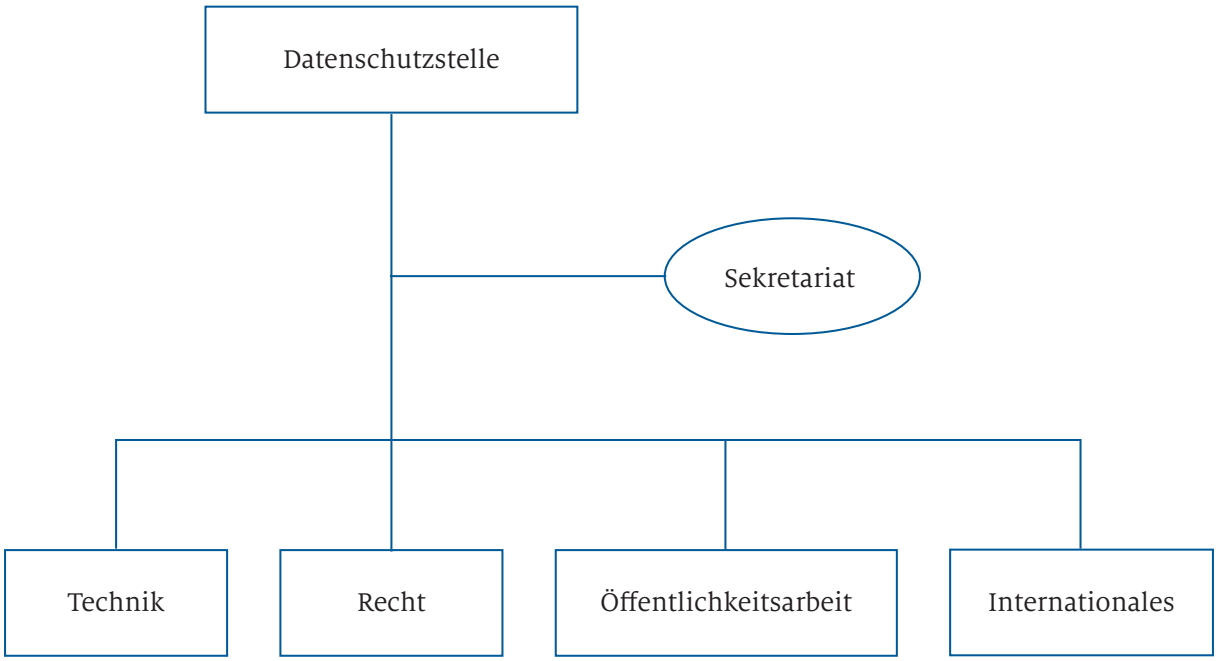
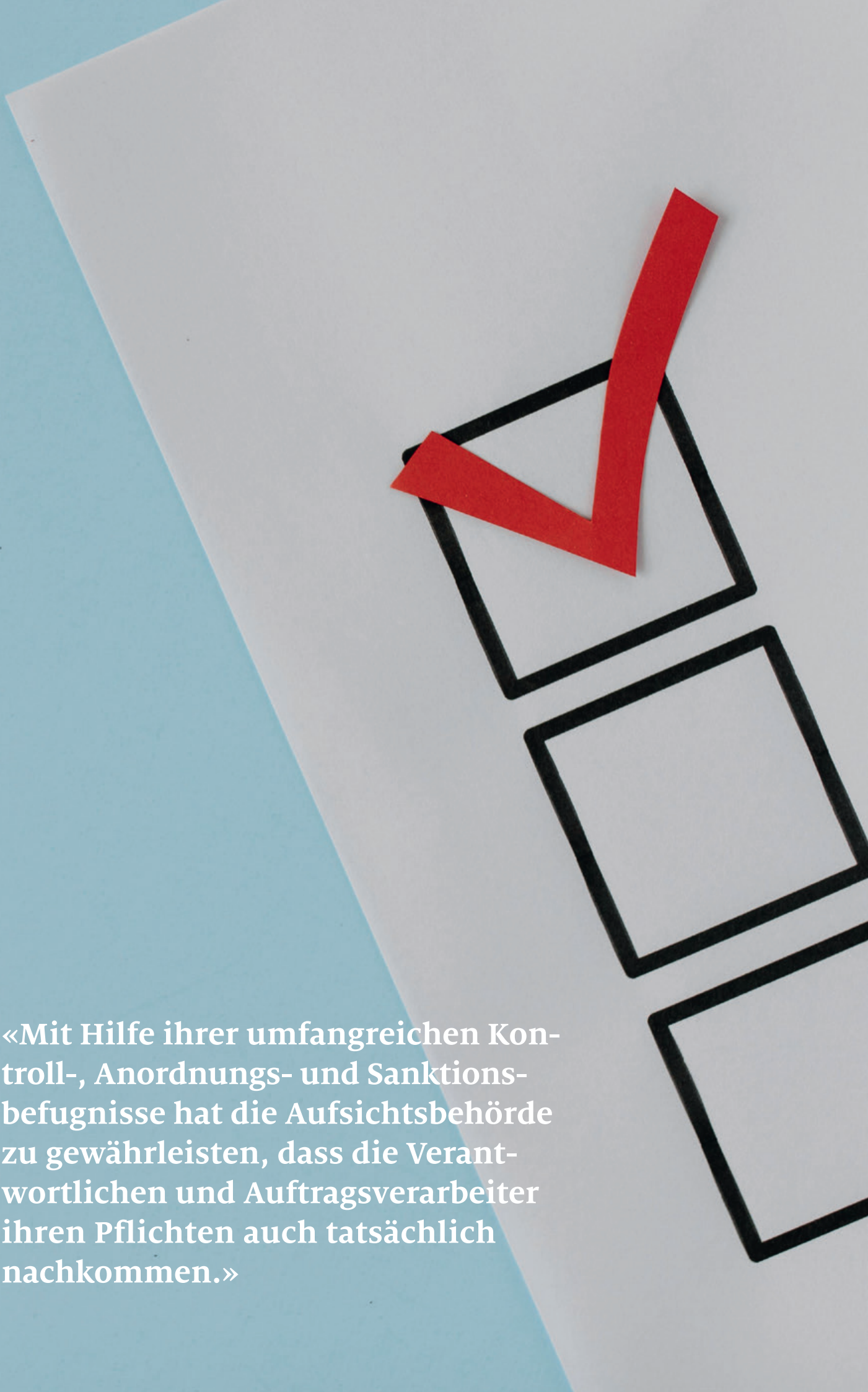


Abbildung 3: Organigramm Datenschutzstelle



«Mit Hilfe ihrer umfangreichen Kontroll-, Anordnungs- und Sanktionsbefugnisse hat die Aufsichtsbehörde zu gewährleisten, dass die Verantwortlichen und Auftragsverarbeiter ihren Pflichten auch tatsächlich nachkommen.»

5. Aufsicht, Beschwerden und Meldungen von Datenschutzverletzungen

5.1 Aufsicht

Die DSGVO nimmt die Verantwortlichen und Auftragsverarbeiter klar in die Pflicht und verlangt, dass sie die Rechte der betroffenen Personen respektieren und ihre diesbezüglichen Verpflichtungen erfüllen. Sie vertraut dabei jedoch nicht allein auf die Eigenverantwortung der Verantwortlichen und Auftragsverarbeiter, sondern erachtet darüber hinaus die Aufsicht als unabdingbar. Gemäss Art. 57 Abs. 1 Bst. a DSGVO muss die Aufsichtsbehörde die Anwendung dieser Verordnung überwachen. Dazu soll die Behörde nach Bst. h «Untersuchungen über die Anwendung dieser Verordnung durchführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde». Im Rahmen einer solchen Untersuchung stehen der Aufsichtsbehörde alle in Art. 58 Abs. 1 DSGVO genannten Untersuchungsbefugnisse zur Verfügung.

Mit Hilfe umfangreicher Kontroll-, Anordnungs- und Sanktionsbefugnisse hat die Aufsichtsbehörde ausserdem zu gewährleisten, dass die Verantwortlichen und Auftragsverarbeiter ihren Pflichten auch tatsächlich nachkommen. Die Befugnisse gehen weiter als unter der vor dem 25. Mai 2018 geltenden Rechtslage und konzentrieren sich auf die in Art. 58 Abs. 2 DSGVO genannten Abhilfemassnahmen sowie die Sanktionsmöglichkeiten nach Art. 83 DSGVO.

Wie bereits in den vergangenen Jahren musste die DSS auch im Berichtsjahr feststellen, dass die aktuellen Personalressourcen für umfassende amtswegige Überprüfungen bei Unternehmen nicht ausreichen. Folglich wurde erneut entschieden, amtswegige Überprüfungen nur anlassbezogen durchzuführen, wenn die DSS klare Hinweise erhält oder ihr anderweitig bekannt wird, dass in einem Unternehmen oder einer öffentlichen Stelle bestimmte Datenverarbeitungsvorgänge nicht gesetzeskonform durchgeführt wurden. Die DSS hat auf diese Weise bei acht privaten und einer öffentlichen Organisation spezifische Untersuchungen aufgrund von konkreten Anlassfällen durchgeführt. Dies sind zwei mehr als im Vorjahr. Dabei wurde jeweils Hinweisen oder Anzeichen dafür nachgegangen, dass bei den Organisationen unzulässige Datenverarbeitungen stattgefunden haben.

Darüber hinaus konnten im Berichtsjahr mehrere bereits 2024 von Amtes wegen, aber auch von Gesetzes wegen, eröffnete datenschutzrechtliche Überprüfungen abgeschlossen werden.

5.1.1 Amtswegige Überprüfungen bei Unternehmen

Nachfolgend wird ein Beispiel der im Berichtsjahr von der DSS vorgenommenen anlassbezogenen amtswegigen Datenschutzüberprüfungen bei Unternehmen vorgestellt.

Amtswegige Überprüfung bei einer Eventagentur

Im Berichtsjahr wurde bei einer Eventagentur eine datenschutzrechtliche Prüfung eingeleitet. Das Unternehmen hat bei der Veranstaltung von grösseren Anlässen ohne Einwilligung der Betroffenen umfassende Teilnehmerlisten im Internet veröffentlicht sowie teilweise diese Listen auch in Papierform ausgeteilt. Die Verantwortliche stützte die Veröffentlichung auf ein berechtigtes Interesse nach Art. 6 Abs. 1 Bst. f DSGVO (Förderung von Austausch und vorgängige Vernetzung), was grundsätzlich zulässig sein könnte. Die DSS verneinte jedoch die Erforderlichkeit, da eine Teilnehmerliste weder absolut notwendig noch das mildeste Mittel ist. Vernetzung vor einer Veranstaltung ist zudem nicht zentraler Zweck einer Veranstaltung. Während der Veranstaltung könnte die Vernetzung vor allem durch weniger eingriffsintensive Massnahmen, wie etwa mittels Namensschilder, gewährleistet werden. Diese sind üblicher, freiwillig nutzbar und effektiver. Auch der Hinweis, die Daten seien teils öffentlich zugänglich, rechtfertigte keine Weiterverarbeitung für eigene Zwecke. Teilnehmende müssen zudem nicht damit rechnen, dass ihre Teilnahme veröffentlicht wird. Folglich stellte die DSS fest, dass die Bereitstellung oder Veröffentlichung von Teilnehmerlisten nur mit wirksamer Einwilligung nach Art. 6 Abs. 1 Bst. a i.V.m. Art. 7 DSGVO zulässig ist; auch ausgedruckte Listen vor Ort lösen das Problem ohne Einwilligung nicht.

5.1.2 Amtswegige Überprüfung bei öffentlichen Stellen

Wie bei privaten Unternehmen hat die DSS im Berichtsjahr auch bei öffentlichen Stellen Datenschutz-Überprüfungen von Amtes wegen vorgenommen. Bereits in Kapitel 2.2. ausgeführt wurde die Datenschutz-Überprüfung einer Videoüberwachung der Landespolizei. Daneben prüfte die DSS etwa beim Schulamt die datenschutzrechtliche Zulässigkeit einer bestimmten Aufsichtspraxis.

Amtswegige Überprüfung beim Schulamt

Nach Hinweisen von Eltern untersuchte die DSS im Berichtsjahr die datenschutzrechtliche Zulässigkeit von Zugriffen durch Lehrpersonen auf Chatnachrichten, die von Schülerinnen und Schülern über die schulischen Computer verfasst wurden und private Inhalte aufwiesen. Gegenstand der Überprüfung war insbesondere, ob und unter welchen Voraussetzungen ein solcher Zugriff – etwa zu Aufsichts-, Sicherheits- oder Disziplinarzwecken – mit den einschlägigen datenschutzrechtlichen Vorgaben sowie dem Schutz der Privatsphäre der betroffenen Schülerinnen und Schüler vereinbar ist. Die DSS kam zum Schluss, dass die Massnahmen nicht unbedingt erforderlich waren zur Erfüllung der gesetzlichen Aufsichtspflichten und vor allem durch gelindere, weniger eingriffsintensive Massnahmen derselbe Zweck erreicht werden könnte. Zusätzlich mussten Schülerinnen und Schüler mangels transparenter Informationen gemäss Art. 13 DSGVO nicht mit solchen Eingriffen in die Privatsphäre rechnen. Ebenso wenig war zum Zeitpunkt der Überprüfung die private Nutzung gänzlich untersagt, weshalb die Aufsichtspersonen davon ausgehen mussten, dass sich unter den eingesehenen Nachrichten auch vereinzelte zulässige private Nachrichten befinden können.

5.1.3 Aufsicht über Videoüberwachungsanlagen

Im Bereich der Videoüberwachung zeigte sich erneut, dass die Abgrenzung zwischen einer unverbindlichen Beratung und einer formellen Beschwerde – insbesondere im nachbarschaftlichen Kontext – für betroffene Personen häufig unklar ist. Die DSS trägt diesem Umstand Rechnung, indem sie auch informelle Eingaben entgegennimmt, den Sachverhalt vorab klärt und zunächst auf eine einvernehmliche Lösung hinwirkt, bevor ein formelles Aufsichtsverfahren eingeleitet wird.

Während im Vorjahr sämtliche Anliegen im Rahmen von Gesprächen und Vor-Ort-Begehungen bereinigt werden konnten, führten im Berichtsjahr insbesondere zwei eskalierte Nachbarschaftskonflikte zu einem erheblichen Mehraufwand. Die Parteien reichten wiederholt formelle Beschwerden gegeneinander ein, was bereits im Stadium der Sachverhaltsermittlung umfangreiche Abklärungen, Stellungnahmen und Dokumentationen erforderte. Am Ende des Berichtsjahres standen in diesen Verfahren noch drei Verfügungen aus. In einem der Fälle war zusätzlich ein Drohnenflug mit Kamerafunktion Gegenstand der Prüfung.

In materiell-rechtlicher Hinsicht betreffen die Streitigkeiten regelmässig dieselben Kernfragen: Erfasst die Kamera öffentlich zugängliche Bereiche, etwa Strassen oder Gehwege, oder richtet sie sich auf Nachbargrundstücke? Die datenschutzrechtliche Beurteilung ist konstant. Videoüberwachungen im rein privaten Bereich sind zulässig, sofern sie sich auf das eigene Grundstück beschränken und weder öffentlich zugängliche Flächen noch benachbarte Liegenschaften erfassen. Sobald jedoch eine solche Erfassung erfolgt, fehlt es an einer tragfähigen Rechtsgrundlage. Auf die spezifische Problematik von Mehrfamilienhäusern wurde in Kapitel 2.2 gesondert eingegangen.

Sowohl bei einvernehmlich gelösten Konflikten als auch im Anschluss an formelle aufsichtsrechtliche Verfahren unterstützt die DSS die Beteiligten bei der datenschutzkonformen technischen und organisatorischen Anpassung bestehender Anlagen.

Erfahrungsgemäss steht bei nachbarschaftlichen Auseinandersetzungen, in denen eine Videoüberwachung Anlass für die Einschaltung der DSS ist, nicht selten ein tieferliegender persönlicher Konflikt im Vordergrund. Die Videoüberwachung fungiert dabei als Auslöser oder Verstärker bestehender Spannungen. Die Lösung solcher Grundsatzkonflikte fällt jedoch nicht in die Zuständigkeit der DSS, deren Mandat sich auf die datenschutzrechtliche Beurteilung beschränkt.

5.1.4 Überprüfungen von Gesetzes wegen

Eine datenschutzrechtliche Überprüfung des Einsatzes der europäischen IT-Systeme Schengener Informationssystem (SIS) und Visa Informationssystem (VIS) durch die Landespolizei und das Ausländer- und Passamt wurde bereits im Vorjahr initiiert. Die Überprüfung des Einsatzes des VIS konnte im Berichtsjahr noch nicht vollständig abgeschlossen werden, diejenige des Einsatzes des SIS hingegen schon. Beim SIS handelt es sich um ein europaweites Fahndungssystem. Ausschreibungen erfolgen grundsätzlich über ein SIRENE-Büro. Dieses ist in Liechtenstein bei der Landespolizei angegliedert. Auch in der täglichen Arbeit der Landespolizei ergeben sich zahlreiche Berührungspunkte mit dem SIS. So waren auch Zugriffskonzepte, Informationspflichten, Protokollierung und Selbstkontrolle der Landespolizei, der Umgang mit Auskunftsbegehren, vertragliche Regelungen mit Auftragsdatenverarbeitern wie auch von der Kriminaltechnik zur Fahndung ausgeschriebene Tatortspuren mutmasslicher Täter im Fokus der datenschutzrechtlichen Überprüfung. Im Rahmen dieser Überprüfung kam die DSS unter anderem zum Schluss, dass Datenweitergaben ans Landesarchiv auf Grund der Überschreitung der maximalen Speicherfristen aus EU-Verordnungen unzulässig sind und die implementierte Protokollierung und Selbstkontrolle

nicht alle Anforderungen erfüllt. Bezüglich der Nutzung von USB-Sticks ist die Vertraulichkeit und der Schutz vor Zugriff Unberechtigter nicht gewährleistet und im Rahmen der Informationspflichten verweist die Landespolizei lediglich auf die Internetseite der DSS, was nicht den gesetzlichen Voraussetzungen entspricht. Darüber hinaus ist jedoch auch festzuhalten, dass die Landespolizei um einen hohen Datenschutzstandard bemüht ist und die DSS die überaus kooperative und gute Zusammenarbeit schätzt.

5.1.5 Schengen-Evaluationen im In- und Ausland

Die gesetzlichen Grundlagen der verschiedenen EU-Informationssysteme im Schengen-Raum schreiben vor, dass deren nationale Implementierung und Nutzung alle sieben Jahre einer datenschutzrechtlichen Überprüfung auf europäischer Ebene unterzogen werden. Im Rahmen der Mitgliedschaft Liechtensteins im Schengen-Raum beteiligte sich die DSS im Berichtsjahr an einer solchen europäischen Evaluierung und entsandte hierfür einen Experten zu einer ersten datenschutzrechtlichen Prüfung eines neuen Mitgliedstaates im Schengenraum.

Wie im Vorjahr schon erwähnt, wird Liechtenstein im Jahr 2026 durch externe Experten, bestehend aus Mitarbeitenden der Europäischen Kommission (EU-Kommission) wie auch anderer EU/EWR-Aufsichtsbehörden, evaluiert werden. Die DSS begann folglich bereits im Sommer 2024, wie durch den Schengen-Acquis gesetzlich gefordert, mit dem Datenschutzaudit beim Ausländer- und Passamt sowie der Landespolizei einschliesslich des SIRENE-Büros. Im Berichtsjahr wurde zudem der umfangreiche Fragebogen, der den Experten zur Vorbereitung der Schengen Evaluation dient, in Zusammenarbeit mit der Landespolizei, dem Ausländer und Passamt und dem Schengen-Koordinator ausgefüllt und eingereicht.

5.2 Beschwerden

Betroffene Personen haben nach Art. 77 DSGVO das Recht, sich bei einer Aufsichtsbehörde zu beschweren, wenn sie der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten nicht rechtmässig erfolgt. Dazu bietet die DSS – wie in Erwägungsgrund 141 der DSGVO empfohlen – auf ihrer Internetseite in der Rubrik «Services» ein elektronisches Beschwerdeformular an. Insgesamt (nationale und internationale) gingen bei der DSS im Berichtsjahr 77 Beschwerden und somit rund 50% mehr als im Vorjahr ein. Von den insgesamt eingelangten Beschwerden richteten sich 11 gegen öffentliche Stellen. Die übrigen Verfahren betrafen Unternehmen und – in einzelnen Fällen – Privatpersonen.

5.2.1 Nationale Beschwerden

Im Berichtsjahr erhielt die DSS insgesamt 72 Beschwerden von Privatpersonen, die sich direkt an die DSS als für ein liechtensteinisches Unternehmen oder eine lokale öffentliche Stelle zuständige Behörde rich-

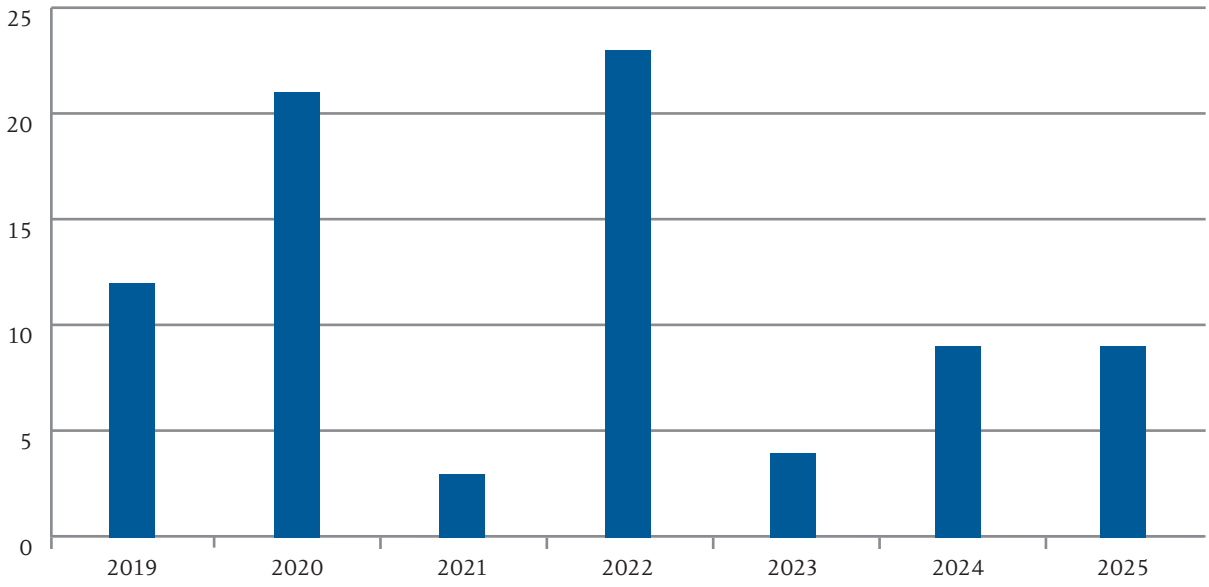


Abbildung 4: Anzahl der Datenschutzüberprüfungen pro Jahr ohne Videoüberwachungen)

teten. Die Beschwerdeführer haben zum überwiegenden Teil ihren Wohnsitz in Liechtenstein. Aber auch Personen aus dem EWR, vor allem aus Deutschland, brachten Beschwerden bei der DSS ein.

Die DSS machte von ihren Befugnissen unter Art. 58 Abs. 2 DSGVO weitreichend Gebrauch und sprach Verwarnungen sowie Anweisungen zur Umsetzung von Betroffenenrechten und zur Herstellung von Rechtskonformität bestimmter Datenverarbeitungen aus. Auch eine Geldbusse von CHF 31'000 wurde im Berichtsjahr gegen ein Unternehmen verhängt, welches einen gravierenden Datenschutzverstoss begangen hatte. Geahndet wurde damit die – entgegen früheren bereits erfolgten Anweisungen der DSS – wiederholte werbliche Kontaktaufnahme mit zahlreichen Personen, ohne dass hierfür eine gültige Rechtsgrundlage im Sinne von Art. 6 Abs. 1 DSGVO vorgelegen hat. Die entsprechende Verfügung ist allerdings noch nicht rechtskräftig.

Inhaltlich konzentrierten sich die Beschwerdeverfahren erneut auf die Betroffenenrechte auf Information, Auskunft, Löschung und Widerspruch sowie die Frage der Rechtmässigkeit einer Datenverarbeitung gemäss Art. 6 Abs. 1 oder Art. 9 Abs. 2 DSGVO. Vermehrt hinzu kamen auch Verletzungen der Sicherheit und Integrität der Daten gemäss Art. 25 DSGVO.

Nicht in allen Beschwerdefällen der DSS bildete eine Verfügung den Abschluss des Verfahrens. Stattdessen konnte in einigen Fällen mit der datenverarbeitenden Stelle (sprich dem verantwortlichen Unternehmen oder der öffentlichen Stelle) eine (einvernehmliche) Lösung gefunden werden, die es erlaubte, die Rechte der Betroffenen zu gewährleisten. Mit diesem auch in Erwägungsgrund 131 der DSGVO empfohlenen Vorgehen konnten im Berichtsjahr erneut einige langwierige und aufwändige Verfahren verhindert werden.

5.2.2 Internationale Beschwerden

Art. 56 Abs. 1 DSGVO bestimmt, dass die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters im EU/EWR-Raum die zuständige federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Datenverarbeitung ist. Wenn eine betroffene Person Beschwerde bei der Aufsichtsbehörde an ihrem Wohnsitz einreicht und diese nicht mit der zuständigen federführenden Aufsichtsbehörde identisch ist, so leitet diese Behörde die Beschwerde an die federführende Behörde im Sitzstaat des Verantwortlichen oder Auftragsverarbeiters weiter. Im Rahmen dieser Zusammenarbeit erhielt die DSS im Berichtsjahr zwei zusätzliche Beschwerden via andere europäische Datenschutz-Aufsichtsbehörden von Personen aus einem anderen EWR-Staat, die sich gegen ein liechtensteinisches Unternehmen richteten. Umgekehrt wurden im Berichtsjahr drei Beschwerden von Personen aus Liechtenstein an andere europäische Datenschutz-Aufsichtsbehörden weitergeleitet.

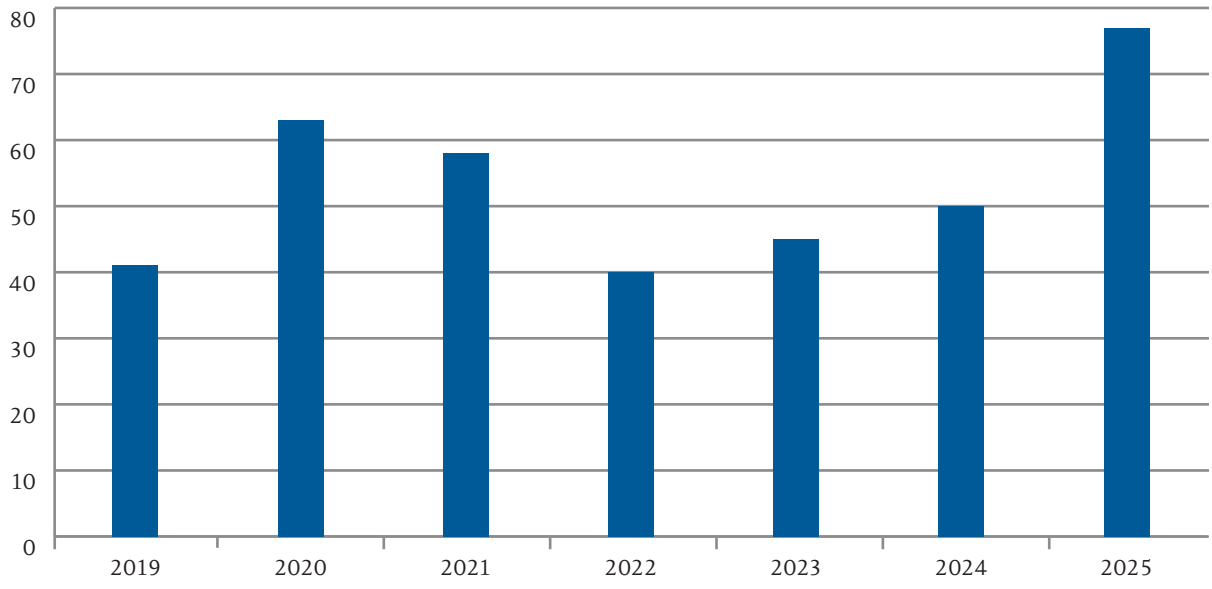


Abbildung 5: Anzahl Beschwerden pro Jahr

5.2.3 Ausgewählte Verfügungen der DSS im Berichtsjahr

Nachdem die Verfügungen der DSS nicht veröffentlicht werden, werden nachfolgend einzelne ausgewählte Entscheidungen der DSS vorgestellt:

Beschwerde betreffend die Einschränkung des Auskunftsgesuches und die Herausgabe von Daten, die freiwillig zur Verfügung gestellt wurden

Ein Beschwerdeführer rügte, ihm sei keine vollständige Auskunft nach Art. 15 Abs. 1 DSGVO erteilt worden; zudem seien nicht sämtliche Datenkopien im Sinne von Art. 15 Abs. 3 DSGVO übermittelt worden. Die verantwortliche Stelle brachte vor, dass die Auskunftsgesuche jeweils thematisch eingegrenzt gewesen seien und sich auf bestimmte Daten oder Verarbeitungsvorgänge bezogen hätten.

Die DSS stellte fest, dass eine verantwortliche Stelle grundsätzlich davon ausgehen darf, dass sich ein Auskunftsersuchen auf jene Daten beschränkt, die von der betroffenen Person im Gesuch konkretisiert oder erkennbar eingegrenzt wurden. Erwägungsgrund 63 DSGVO sieht vor, dass der Verantwortliche bei einer grossen Datenmenge eine Präzisierung des Begehrens verlangen kann. Im vorliegenden Fall hatte jedoch die betroffene Person selbst ihre Gesuche inhaltlich klar auf bestimmte Zwecke oder Sachverhalte beschränkt. Die DSS kam daher zum Schluss, dass eine entsprechende inhaltliche Begrenzung des Auskunftsanspruchs auch ohne formelles Präzisierungsverlangen durch die verantwortliche Stelle zulässig ist, sofern sich die Einschränkung eindeutig aus dem Gesuch ergibt.

In Bezug auf die Auskunft über Daten, welche eine betroffene Person selbst (ohne dass dies erforderlich gewesen wäre) zur Verfügung gestellt hat, stellte die DSS fest: Nach den Leitlinien 01/2022 des EDSA zum Auskunftsrecht (Rn. 19) umfasst das Auskunftsrecht nach Art. 15 Abs. 1 DSGVO die Mitteilung der konkret verarbeiteten personenbezogenen Daten selbst und nicht lediglich eine allgemeine Beschreibung oder die Angabe von Datenkategorien. Der Anspruch besteht grundsätzlich hinsichtlich aller verarbeiteten personenbezogenen Daten, unabhängig von deren Art oder Herkunft. Dies gilt ausdrücklich auch für Daten, welche die betroffene Person dem Verantwortlichen ursprünglich selbst zur Verfügung gestellt hat. Zweck der Auskunft ist es, der betroffenen Person Transparenz über die tatsächliche Verarbeitung ihrer Daten zu verschaffen. Der Verantwortliche wurde entsprechend von der DSS angewiesen, die Auskunft diesbezüglich noch zu vervollständigen. Die Verfügung ist allerdings noch nicht rechtskräftig.

Beschwerde betreffend Cookie-Banner

Der Beschwerdeführer brachte vor, dass der auf einer Internetseite eingesetzte Cookie-Banner die Datenschutzerklärung ganz oder teilweise verdeckte und damit den Zugang zu den nach Art. 13 DSGVO erforderlichen Informationen erschwerte. Nach Art. 13 DSGVO sind betroffene Personen zum Zeitpunkt der Datenerhebung umfassend über Art, Zweck und Rechtsgrundlagen der Verarbeitung zu informieren. Art. 12 DSGVO verlangt zudem eine transparente, verständliche und leicht zugängliche Bereitstellung dieser Informationen. Die DSS stellte daher fest, dass ein Cookie-Banner, welcher die Datenschutzerklärung überlagert oder blockiert, diesen Anforderungen nicht genügt. Wird der Zugang zu den Informationen im Zeitpunkt der Datenerhebung faktisch verhindert oder erheblich erschwert, fehlt es an der notwendigen Transparenz. Eine unter solchen Umständen eingeholte Einwilligung kann nicht als «informiert» gelten und ist folglich unwirksam.

Zum Einsatz von Cookies stellte die DSS fest, dass dieser entweder auf eine Einwilligung (Art. 6 Abs. 1 Bst. a DSGVO) oder auf berechtigte Interessen (Art. 6 Abs. 1 Bst. f DSGVO) und in selteneren Fällen auf einen Vertrag (Art. 6 Abs. 1 Bst. b DSGVO) gestützt werden muss. Massgeblich ist die Funktion der jeweiligen Cookies. Nicht funktionale Cookies – insbesondere Tracking- und Analysedienste zu Marketing- oder Profilingzwecken – erfordern grundsätzlich eine ausdrückliche Einwilligung, da die Interessen der Betroffenen am Schutz ihrer Privatsphäre überwiegen. Technisch notwendige Cookies oder solche zur anonymisierten Reichweitenmessung können hingegen auf berechtigte Interessen gestützt werden, sofern die Grundprinzipien der DSGVO eingehalten werden. Zudem müssen einwilligungspflichtige Cookies standardmässig blockiert bleiben, bis eine aktive Zustimmung erfolgt. Das heisst, dass bereits bei der Einholung der Einwilligung – etwa über eine Consent-Management-Plattform (CMP) – sicherzustellen ist, dass keine Daten verarbeitet werden, die ihrerseits einer vorgängigen Einwilligung bedürfen. Die CMP darf ausschliesslich solche personenbezogenen Daten erheben und verarbeiten, die für das Einwilligungsmanagement technisch zwingend erforderlich sind (Grundsatz der Datenminimierung). Der Verantwortliche hat daher die eingesetzte Lösung auf die strikte Einhaltung dieser Anforderungen zu überprüfen und gegebenenfalls datenschutzkonform zu konfigurieren. Ist eine entsprechende Anpassung nicht möglich, ist eine datenschutzkonforme Alternative einzusetzen.

Beschwerde betreffend Nutzung von Grundbuchdaten zu kommerziellen Zwecken

In diesem Fall war zu prüfen, ob ein Unternehmen personenbezogene Daten aus dem öffentlich zugänglichen Grundbuch erheben und für kommerzielle Zwecke verwenden darf. Die DSS stellte fest, dass die Datenerhebung ausnahmsweise zulässig ist und auch die Verarbeitung zur einmaligen Kontaktaufnahme mit Grundstückseigentümern auf Art. 6 Abs. 1 Bst. f DSGVO (berechtigtes Interesse) gestützt werden kann. Die Interessenabwägung ergibt, dass das wirtschaftliche Interesse legitim ist, die Verarbeitung im Sinne einer einmaligen gezielten Kontaktaufnahme mit einem Grundstücks-/Hauseigentümer zur Zielerreichung erforderlich ist und die Interessen der betroffenen Personen angesichts der öffentlichen Zugänglichkeit der Daten sowie der Begrenzung auf eine einmalige Kontaktaufnahme nicht überwiegen. Eine vorgängige Geschäftsbeziehung ist hierfür nicht erforderlich.

Zulässig ist jedoch lediglich ein einmaliges, transparentes Anschreiben an die Eigentümer. Für weitergehende Kontaktaufnahmen ist grundsätzlich eine Einwilligung erforderlich, sofern sich aus dem Erstkontakt keine vertragliche Beziehung ergibt. Aus diesem Grund reichte in dem speziellen Fall ein sogenanntes Opt-out im Sinne eines Widerspruchsrechts gemäss Art. 21 DSGVO nicht, sondern hätte im ersten Anschreiben eine Einwilligung für eine wiederholte Kontaktaufnahme eingeholt werden müssen. Folglich erfolgten alle weiteren Anschreiben rechtswidrig unter Verletzung des Art. 6 Abs. 1 DSGVO. Die Verfügung ist allerdings noch nicht rechtskräftig.

Beschwerde betreffend die praktische Geltendmachung von Betroffenenrechten

Ein Beschwerdeführer machte geltend, sein per E-Mail an die auf der Internetseite angegebene Adresse übermitteltes Auskunftsgesuch nach Art. 15 DSGVO sei von der verantwortlichen Stelle nicht beantwortet worden. Im Verfahren stellte sich heraus, dass die E-Mail aufgrund eines technischen Problems nicht zugestellt wurde. Die verantwortliche Stelle bestätigte diesen Umstand.

Die DSS gab der Beschwerde statt und stellte fest, dass ungeachtet der technischen Ursache eine Verletzung von Art. 12 Abs. 2 und 3 i.V.m. Art. 15 DSGVO vorliegt, da das Auskunftsersuchen nicht fristgerecht beantwortet wurde. Entscheidend ist nicht das Verschulden, sondern die objektive Pflicht zur Gewährleistung einer ordnungsgemässen Bearbeitung von Betroffenenanfragen. Unter Verweis auf Erwägungsgrund 63 DSGVO betonte die DSS, dass betroffene Personen ihr Auskunftsrecht «problemlos» und effektiv ausüben können müssen, um sich der Datenverarbeitung bewusst sein und deren Rechtmässigkeit überprüfen zu können. Art. 12 Abs. 2 DSGVO verpflichtet Verantwortliche ausdrücklich, die Ausübung der Betroffenenrechte zu erleichtern. Dazu gehört insbesondere die Sicherstellung eines funktionierenden, verlässlichen und regelmässig überprüften Kommunikationskanals, über den entsprechende Gesuche entgegengenommen und bearbeitet werden können.

Beschwerde betreffend die Weitergabe personenbezogener Daten an Dritte ohne Bevollmächtigung

Eine betroffene Person hat im Berichtsjahr eine Beschwerde gegen eine öffentliche Stelle eingereicht. Sie brachte vor, dass eine Verfügung der öffentlichen Stelle ohne ihre Einwilligung an eine Drittperson versandt wurde. Die verantwortliche Stelle führte in ihrer Stellungnahme aus, dass eine Vollmacht für spezifische Geschäftsbereiche vorläge, und reichte diese bei der DSS ein. Die Vollmacht war zwar nur von der Vollmachtgeberin, jedoch nicht von der bevollmächtigten Person unterschrieben worden, wurde jedoch von letzterer per E-Mail der verantwortlichen Stelle übermittelt. Es stellte sich daher die Frage, ob mit dieser unvollständigen Vollmacht trotzdem eine gültige Rechtsgrundlage im Sinne von Art. 6 Abs. 1 und Art. 9 Abs. 2 DSGVO für die Weiterleitung der Verfügung vorlag. Die DSS kam in ihrer Beurteilung zum Schluss, dass es sich bei der Vollmacht um einen Bevollmächtigungsvertrag (nach § 1002 ff. ABGB) zwischen der Vollmachtgeberin, der Bevollmächtigten und der öffentlichen Stelle handelt. Dabei ist eine Willenserklärung aller Parteien erforderlich. Obwohl die Bevollmächtigte den Bevollmächtigungsvertrag nicht unterzeichnete, konnte festgestellt werden, dass der Versand der Vollmacht eine solche Willensbekundung darstellt. Somit liegt eine gültige Rechtsgrundlage nach Art. 6 Abs. 1 Bst. b DSGVO vor. Weiters wurde aus datenschutzrechtlicher Sicht festgestellt, dass die Vollmacht mit der alleinigen Unterschrift der Vollmachtgeberin auch als Einwilligung zu einer Datenweitergabe im Sinne von Art. 6 Abs. 1 Bst. a ebenso wie Art. 9 Abs. 2 Bst. a DSGVO verstanden werden kann. Für die Einwilligung bedarf es lediglich der klaren Bekundung des Einverständnisses der betroffenen Person. Mit ihrer Unterschrift auf der Vollmacht hat sie klar zum Ausdruck gebracht, dass sie einer Offenlegung der Daten an die in der Vollmacht bezeichnete Person zustimmt. Nachdem der Vollmachtgeberin auch klar war, dass die Datenverarbeitung durch die öffentliche Stelle sensible Daten im Sinne des Art. 9 Abs. 1 DSGVO umfasste, konnte ihre Unterschrift sowohl als Einwilligung im Sinne des Art. 6 Abs. 1 Bst. a (für «normale»

Daten) sowie Art. 9 Abs. 2 Bst. a DSGVO (für Gesundheitsdaten) qualifiziert werden.

5.2.4 Entscheidungen der Beschwerdekommission für Verwaltungsangelegenheiten (VBK)

Im Berichtsjahr entschied die VBK über vier Beschwerden, welche von einer der beiden Verfahrensparteien gegen Verfügungen der DSS eingebracht worden waren. In zwei Fällen bestätigte die VBK die Entscheidungen der DSS. In den zwei weiteren Fällen wurde die Beschwerde verworfen. Insgesamt sind noch vier weitere Beschwerden bei der VBK hängig.

5.2.5 Beschwerden an den Verwaltungsgerichtshof (VGH)

Der VGH entschied im Berichtsjahr über zwei inhaltsgleiche Beschwerden aus dem Vorjahr und hiess beide gut. Streitgegenstand war die Frage, ob eine Anwaltskanzlei im Rahmen eines gerichtlichen Verfahrens verpflichtet war, in einer Eingabe an das Gericht den Namen eines Mitarbeitenden einer inländischen Aufsichtsbehörde zum Schutz von dessen Privatsphäre zu schwärzen. Die DSS sowie die VBK vertraten die Auffassung, dass die namentliche Nennung des Mitarbeitenden für die sachgerechte Vertretung der Mandantschaft nicht zwingend erforderlich war. Da die Identität für die rechtliche Argumentation keine entscheidende Rolle spielte, wäre eine Anonymisierung oder zumindest eine Reduktion auf die Funktionsbezeichnung ausreichend gewesen. Entsprechend qualifizierten sie die vollständige Namensnennung als unverhältnismässige Verarbeitung personenbezogener Daten. Der VGH folgte dieser Argumentation nicht.

Zudem wurde in zwei weiteren Fällen Beschwerde gegen Entscheidungen der DSS bzw. der VBK beim VGH erhoben, wovon der VGH in einem Fall die Entscheidung der DSS bestätigte, der zweite Fall jedoch nach wie vor hängig ist.

5.2.6 Beschwerden an den Staatsgerichtshof (StGH)

Im Berichtsjahr wurde ausserdem eine Individualbeschwerde beim StGH gegen eine Verfügung der DSS bzw. das bestätigende Urteil des VGH erhoben. Dieser Beschwerde wurde vom StGH jedoch keine Folge gegeben.

5.3 Meldung von Datenschutzverletzungen gemäss Art. 33 DSGVO

Art. 33 DSGVO verpflichtet Verantwortliche, Verletzungen des Schutzes personenbezogener Daten der zuständigen Datenschutz-Aufsichtsbehörde binnen 72 Stunden zu melden, wenn aufgrund der Verletzung voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Überdies müssen die betroffenen Personen gemäss Art. 34 DSGVO unverzüglich benachrichtigt werden, wenn voraussichtlich ein hohes Risiko für ihre Rechte und Freiheiten zu erwarten ist. Verzögerte oder unterlassene Benachrichtigungen konterkarieren den präventiven Schutzzweck der DSGVO. Die Informationspflicht dient dazu, betroffenen Personen frühzeitig Transparenz über eine Datenschutzverletzung zu verschaffen, damit sie konkrete Schutzmassnahmen ergreifen können, etwa die Sperrung von Zahlungsinstrumenten, die Änderung von Zugangsdaten oder eine erhöhte Wachsamkeit gegenüber Phishing- und Betrugsversuchen. Erfolgt die Mitteilung nicht unverzüglich, verlieren Betroffene dieses kritische Zeitfenster. Dadurch steigt das Risiko von Identitätsdiebstahl, unbefugten Transaktionen, Reputationsschäden oder sonstigen finanziellen und immateriellen Nachteilen erheblich.

Im Berichtsjahr gingen bei der DSS insgesamt 77 Meldungen über Verletzungen des Schutzes personenbezogener Daten gemäss Art. 33 DSGVO ein. Gegenüber dem Vorjahr mit 57 Meldungen entspricht dies einer signifikanten Steigerung um rund 35 %. Im Vorjahr war lediglich in 19 Fällen zusätzlich eine Benachrichtigung der betroffenen Personen nach Art. 34 DSGVO erforderlich. In den im Berichtsjahr bislang abgeschlossenen Verfahren wurde in 41 Fällen eine Benachrichtigung der betroffenen Personen vorgenommen. Damit lag in mehr als der Hälfte der Fälle ein voraussichtlich hohes Risiko für die Rechte und Freiheiten der betroffenen Personen vor. Neben der Meldepflicht gegenüber der Aufsichtsbehörde bestand folglich auch eine unmittelbare Informationspflicht gegenüber den Betroffenen.

Die im Berichtsjahr gemeldeten «klassischen» Datenschutzverletzungen betrafen überwiegend organisatorische und manuelle Fehlerquellen. Dazu zählten insbesondere E-Mails an unzutreffende Empfänger, vertauschte oder falsch adressierte Postsendungen, fehlerhafte Dokumentenanhänge, Tippfehler in E-Mail-Adressen, irrtümliche Weiterleitungen oder unbefugte Einsichtnahmen sowie unzutreffend vergebene Zugriffs- und Berechtigungsrechte in IT-Systemen. Auch ein einmaliger Fehlversand personenbezogener Daten begründet regelmässig ein relevantes Risiko für die betroffenen Personen, insbesondere, wenn sensible Identifikations-, Finanz- oder Vertragsdaten betroffen sind. Solche Vorfälle können Identitätsmissbrauch, Vermögensschäden oder Reputationsbeeinträchtigungen nach sich ziehen und er-

fordern daher stets eine strukturierte Risikobewertung im Einzelfall.

Parallel dazu nahmen die gemeldeten Cybervorfälle nicht nur zahlenmässig zu, sondern zeigten auch eine deutlich höhere technische und organisatorische Komplexität. Angreifer nutzten gezielte Phishing-Kampagnen, um Zugangsdaten abzugreifen und E-Mail-Konten zu kompromittieren. Nach erfolgreicher Übernahme wurden aus den betroffenen Accounts weitere Phishing-Nachrichten versendet. Da diese Nachrichten vom tatsächlichen E-Mail-Konto der betroffenen Organisation ausgingen, wirkten sie gegenüber Kunden, Geschäftspartnern und weiteren Kontaktpersonen besonders glaubwürdig. Dadurch erweiterte sich der Kreis potenziell Betroffener erheblich und das Schadenspotenzial stieg deutlich an. Bereits der Verlust von Zugangsdaten oder die Kompromittierung eines E-Mail-Kontos stellt für sich genommen ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen dar, sowohl der eigentlichen Kontoinhaber, aber eben auch für sämtliche damit unrechtmässigerweise kontaktierten Personen. In solchen Konstellationen ist regelmässig eine unverzügliche Benachrichtigung gemäss Art. 34 DSGVO erforderlich, damit Betroffene zeitnah Schutzmassnahmen ergreifen können, etwa die Änderung von Passwörtern, erhöhte Wachsamkeit gegenüber betrügerischen Nachrichten oder die Absicherung weiterer Zugänge, um Folgeschäden zu minimieren.

Zusätzlich meldeten Verantwortliche vermehrt Vorfälle, bei denen Absenderadressen technisch gefälscht (Spoofing) oder E-Mail-Inhalte während der Übertragung manipuliert wurden. Diese Nachrichten waren teilweise kaum von legitimer Geschäftskorrespondenz zu unterscheiden und führten vereinzelt zu finanziellen Schäden oder zur unbefugten Offenlegung weiterer personenbezogener Daten mit teils erheblichen Folgewirkungen.

Spezielle Aufmerksamkeit erforderten Vorfälle, bei denen besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO betroffen waren, wie insbesondere Gesundheitsdaten, oder auch umfangreiche Finanzinformationen. Aufgrund ihres erhöhten Missbrauchs-, Diskriminierungs- und Reputationsschädigungspotenzials ist in solchen Konstellationen regelmässig von einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen auszugehen. Entsprechend bestand in all diesen Fällen eine Pflicht zur unverzüglichen Benachrichtigung nach Art. 34 DSGVO.

Ein wesentlicher Anteil der gemeldeten Datenschutzverletzungen stand im Zusammenhang mit Auftragsverarbeitern, insbesondere im IT- und Cloud-Umfeld sowie bei komplexen, arbeitsteiligen Verantwortungsstrukturen. Verzögerte, unvollständige oder technisch schwer nachvollziehbare Informationen seitens des Auftragsverarbeiters erschweren die fristgerechte Meldung an die Aufsichtsbehörde nach

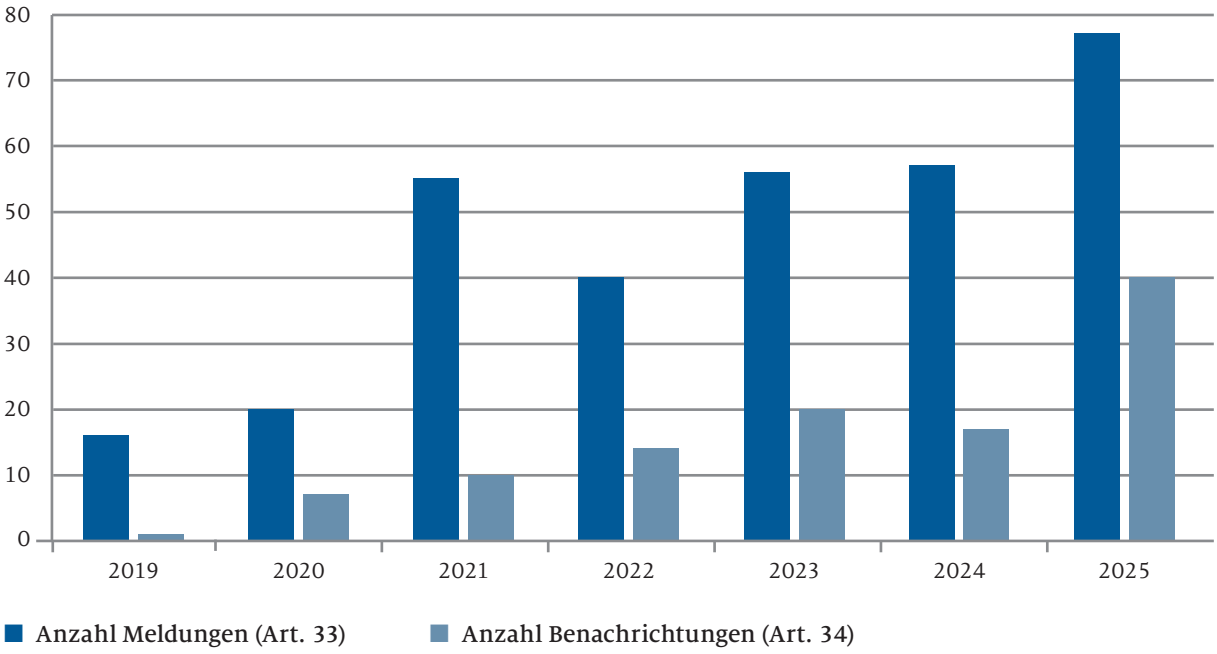


Abbildung 6: Anzahl der gemeldeten Datenschutzverletzungen pro Jahr

Art. 33 DSGVO und die fundierte Entscheidung über eine Benachrichtigung der betroffenen Personen nach Art. 34 DSGVO. Dies verdeutlicht die zentrale Bedeutung der vertraglichen und gesetzlichen Mitwirkungs-, Informations- und Unterstützungspflichten des Auftragsverarbeiters. Er muss dem Verantwortlichen Sicherheitsvorfälle unverzüglich anzeigen, sämtliche relevanten Informationen bereitstellen und aktiv an der Sachverhaltsaufklärung sowie an der Risikobewertung mitwirken.

Vor diesem Hintergrund sind belastbare organisatorische und technische Strukturen entscheidend. Ein wirksames Datenschutz-Managementsystem umfasst klare interne Zuständigkeiten, definierte Melde- und Eskalationsprozesse, die frühzeitige Einbindung des Datenschutzbeauftragten, regelmässige Schulungen der Mitarbeitenden sowie angemessene technische und organisatorische Massnahmen. Dazu zählen insbesondere Verschlüsselung, Mehr-Faktor-Authentifizierung, restriktive Berechtigungskonzepte, Protokollierungssysteme und Incident-Response-Pläne. Nur durch solche strukturierten Vorkehrungen lassen sich die Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO fristgerecht erfüllen und hohe Risiken frühzeitig erkennen sowie wirksam begrenzen.

«Die DSS beriet diverse Stellen zu Einzelfragen in verschiedenen Gesetzgebungsprozessen.»

6. Mitarbeit in Arbeitsgruppen, Projekten und Kommissionen der Landesverwaltung

6.1 Arbeitsgruppe «M365-Copilot»

Im Jahr 2025 wurde eine Arbeitsgruppe zur Ausarbeitung eines Grundlagenpapiers für den rechtskonformen und den Anforderungen an die Informationssicherheit entsprechenden Einsatz der KI-Anwendung «M365-Copilot» von Microsoft in der LLV lanciert. Im Rahmen dieser fachübergreifenden Arbeitsgruppe wurde die DSS ersucht, sich an der Ausarbeitung dieses Grundlagenpapiers zu beteiligen. Diesem Ersuchen kam die DSS nach und unterstützte insbesondere bei der Analyse der spezifischen Datenschutzrisiken.

6.2 ZPR-Kommission

Art. 19 des Gesetzes vom 2. Juni 2022 über das Zentrale Personenregister (ZPRG) sieht die Einsetzung einer ZPR-Kommission vor. Im Zuge der Gesetzesrevision wurde die formelle Vertretung der DSS in diesem Gremium aufgehoben, sodass seither kein institutionalisierter Einsitz der DSS mehr vorgesehen ist. In der praktischen Arbeit der Kommission haben sich in den letzten Jahren jedoch vermehrt Rechtsfragen zur Verarbeitung personenbezogener Daten ergeben, insbesondere im Zusammenhang mit der geplanten Anpassung der einschlägigen Verordnung sowie mit Fragen der Rechtmässigkeit, Zweckbindung und Datenzugriffsberechtigungen. Vor diesem Hintergrund wurde die DSS ersucht, wieder regelmässig an den Sitzungen der Kommission teilzunehmen und die Kommission in datenschutzrechtlichen Fragestellungen beratend zu unterstützen.

6.3 Task Force zur Prüfung von Handlungsbedarf und Massnahmen betreffend Datenschutz im schulischen Umfeld

Mit Regierungsbeschluss vom 25. November 2025 setzte die Regierung eine Task Force zur Prüfung von Handlungsbedarf und Massnahmen betreffend Datenschutz im schulischen Umfeld ein. Auftrag des Gremiums ist es, allfälligen Handlungsbedarf zu prüfen und mögliche Massnahmen betreffend Datenschutz im schulischen Umfeld sowie zur Lösung der pendenten Beschwerdefälle zu ergreifen. Die DSS begrüsste die Einsetzung dieses Gremiums ausdrücklich und erklärte ihre Bereitschaft, sich aktiv in die Arbeiten der Task Force einzubringen. Die erste Sitzung erfolgte im Januar 2026.

6.4 Kompetenzgruppe Digitalisierung

Im September 2025 wurde die DSS eingeladen, in der Kompetenzgruppe Digitalisierung beratend mitzuwirken. In diesem Rahmen beteiligte sie sich an der Erarbeitung eines Merkblatts «FAQ zur Nutzung generativer KI in der LLV» sowie an der Ausarbeitung einer übergeordneten KI-Strategie. Aus Sicht der DSS ist dabei eine klare Differenzierung zwischen internen, von der LLV zentral bereitgestellten KI-Tools und externen, frei zugänglichen Anwendungen essenziell. Diese Unterscheidung ist insbesondere im Hinblick auf Datenschutz, Informationssicherheit und Verantwortlichkeiten von Bedeutung. Ein zentrales Ziel der Strategie sollte es zudem sein, die Entstehung einer sogenannten «Schatten-KI» zu verhindern, also einer dezentralen und ungesteuerten Nutzung externer KI-Tools ohne vorgängige Prüfung ihrer rechtlichen und sicherheitstechnischen Konformität.

Die DSS empfiehlt daher die Einrichtung einer zentralen Meldestelle, über die Bedarf angemeldet und Vorschläge für geeignete KI-Tools eingebracht werden können. Ergänzend sollte eine zentrale Beratungsstelle geschaffen werden, die Mitarbeitende in Fragen der datenschutzrechtlichen Zulässigkeit, der rechtlichen Rahmenbedingungen sowie technischer Anforderungen beim Einsatz von KI-Systemen unterstützt.

6.5 Fachstab Cyber – Aufbau einer nationalen Krisenorganisation zur Bewältigung von Cybersicherheitsvorfällen grossen Ausmasses und Krisen

Im September des Berichtsjahres erhielt die DSS die Aufforderung der Stabsstelle Cyber-Sicherheit, eine für juristische und eine für technische Fragen zuständige Person der DSS für den Fachstab Cyber zur Verfügung zu stellen. Die DSS konnte entgegen der Aufforderung jedoch nur eine Person formell für den Fachstab nominieren, da es aufgrund hoher Arbeitsauslastung nicht möglich sein wird, dass zwei Personen der DSS entsprechende Ausbildungen absolvieren und an Sitzungen etc. teilnehmen.

6.6 VwbP-Kommission

Gemäss Art. 27 des Gesetzes vom 3. Dezember 2020 über das Verzeichnis der wirtschaftlich berechtigten Personen von Rechtsträgern (VwbPG) hat die DSS Einsitz in der VwbP-Kommission. Der VwbP-Kom-

mission obliegt die Entscheidung über die Offenlegungsanträge Dritter im Sinne von Art. 17 VwbPG. Im Berichtsjahr wurde ein Antrag gemäss Art. 17 VwbPG betreffend die Offenlegung von Daten an Dritte an das Amt für Justiz gestellt. Der Antrag wurde von der VwbP-Kommission im Januar 2026 entschieden.

6.7 Beratung zu weiteren Gesetzgebungsprozessen

Zusätzlich zu den genannten umfassenden Beratungen beriet die DSS auch diverse weitere Stellen zu Einzelfragen in verschiedenen Gesetzgebungsprozessen. Dies umfasste unter anderem die geplante Anpassung des Datenschutzgesetzes, des Versicherungsaufsichtsgesetzes, des Geldspielgesetzes, des Gesetzes über die Stabsstelle Financial Intelligence Unit oder des Abkommens mit Österreich über die Übernahme von Vollziehungsaufgaben im Zusammenhang mit der EU-Tabakprodukte-Richtlinie 2014/40/EU. Ebenso war die DSS eingebunden in die nationale Umsetzung der EU-Digitalisierungsrechtsakte wie der KI-Verordnung oder des Data Governance Acts.

«Die DSGVO erfordert nicht nur eine Zusammenarbeit der europäischen Datenschutz-Aufsichtsbehörden im bzw. mit dem EDSA, sondern auch eine intensive Kommunikation zwischen den einzelnen Aufsichtsbehörden.»

7. Internationale Zusammenarbeit

7.1 Europäischer Datenschutzausschuss (EDSA)

Eine der Hauptaufgaben des EDSA ist der Erlass von Leitlinien, aber auch die Abgabe von Empfehlungen und Stellungnahmen u.ä., die der einheitlichen Auslegung und Anwendung der DSGVO dienen. Die Grundlagen für diese Dokumente des Ausschusses werden in diversen themenbezogenen Arbeitsgruppen geschaffen, welche die Dokumente für die Abstimmung im Ausschuss vorbereiten. Wie bereits im Vorjahr konnte die DSS auch 2025 an den meisten Sitzungen der Arbeitsgruppen teilnehmen und aktiv mitarbeiten. Die DSS nahm ausserdem an allen zwölf Plenarsitzungen des Ausschusses teil.

7.1.1 Stellungnahmen, Leitlinien und Empfehlungen des EDSA

Der EDSA hat im Jahr 2025 auf Grundlage des **Art. 64 Abs. 1 und 2 DSGVO** insgesamt **28 Stellungnahmen** zu Vorlagen und Fragen von nationalen Datenschutz-Aufsichtsbehörden abgegeben. Darunter fielen:

- drei Stellungnahmen zu je einem Entwurf der Akkreditierungsanforderungen für eine Zertifizierungsstelle gemäss Art. 42 Abs. 5 DSGVO (Frankreich, Griechenland, Österreich);
- 25 Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (Aramex Group, Arcadis Group, ASML Group, zwei zu BOX Group, Coface Group, zwei zu CSG Group, Ferrero Group, zwei zu Illumina Group, Laval Group, Mowi Group, zwei zu Nokia Group, zwei zu Northern Trust Group, zwei zu Shopify Group, Signify Group, Statkraft Group, Tessi Group, Wilhelmsen Group, zwei zu Worldline Group).

Auch hat der EDSA im Berichtsjahr auf Grundlage des **Art. 70 DSGVO** folgende **Stellungnahmen** abgegeben:

- drei Stellungnahmen zu je einem Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäss Art. 45 der Verordnung (EU) 2016 / 679 (DSGVO) über die Angemessenheit des Datenschutzniveaus (Brasilien, Europäische Patentorganisation (EPO), Vereinigtes Königreich);
- eine Stellungnahme zu einem Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäss Art. 36 der Richtlinie (EU) 2016 / 680 (LED) über die Angemessenheit des Datenschutzniveaus (Vereinigtes Königreich);
- eine Stellungnahme zur Erweiterung der Durchführungsbeschlüsse der Europäischen Kommission gemäss der DSGVO und der LED über die Angemessenheit des Datenschutzniveaus (Vereinigtes Königreich).

Zusätzlich haben der EDSA und der Europäische Datenschutzbeauftragte (EDSB) 2025 eine **Gemeinsame Stellungnahme** erlassen:

- Gemeinsame Stellungnahme 01/2025 zum Vorschlag für eine Verordnung über Vereinfachungsmassnahmen für KMUs, insbesondere die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäss Art. 30 Abs. 5 DSGVO.

Die im Berichtsjahr vom EDSA **angenommene Leitlinie** befasst sich mit folgendem Thema:

- Leitlinien zu Artikel 48 DSGVO (EDPB Guidelines 02/2024).

Folgende Leitlinien wurden vom EDSA im Berichtsjahr in die **öffentliche Konsultation** gegeben:

- Leitlinien zur Pseudonymisierung (EDPB Guidelines 01/2025);
- Leitlinien zur Verarbeitung personenbezogener Daten durch Blockchain-Technologien (EDPB Guidelines 02/2025);
- Leitlinien zum Zusammenspiel des Gesetzes über digitale Dienste (DSA) und der DSGVO (EDPB Guidelines 03/2025).

Ausserdem haben der EDSA und die EU-Kommission 2025 eine **Gemeinsame Leitlinie** in die **öffentliche Konsultation** gegeben:

- Gemeinsame Leitlinien zum Zusammenspiel des Gesetzes über digitale Märkte (DMA) und der DSGVO.

Im Berichtsjahr hat der EDSA ausserdem folgende **Empfehlung** verabschiedet:

- Empfehlungen zum Welt-Anti-Doping-Kodex 2027 der WADA (Recommendations 01/2025).

Folgende **Empfehlungen** wurde vom EDSA 2025 in die **öffentliche Konsultation** gegeben:

- Empfehlungen zur Rechtsgrundlage bei der verpflichtenden Erstellung von Nutzerkonten in Online-Shops (Recommendations 02/2025).

7.1.2 Arbeitsgruppen

Wie bereits ausgeführt, beteiligt sich die DSS aktiv an der Arbeit des EDSA zur einheitlichen Anwendung der DSGVO im EU/EWR-Raum. Dazu hat die DSS nicht nur im Ausschuss selbst, sondern auch in diversen seiner Arbeitsgruppen (Expert Subgroups, Taskforces) zu unterschiedlichen Themen Einsitz, welche nachfolgend dargestellt werden. Die Mitarbeitenden der DSS haben 2025 an insgesamt 162 Sitzungen des Ausschusses und solcher Arbeitsgruppen teilgenommen.

Die spezielle Arbeitsgruppe (Task Force) des EDSA zu Bussgeldern gemäss DSGVO *(Taskforce Fining)* befasst sich mit der konkreten Berechnung der Bussgelder und strebt europaweit eine möglichst einheitliche Herangehensweise an. Im Berichtsjahr hat die Arbeitsgruppe die Überarbeitung der Leitlinien der ehemaligen Artikel-29-Datenschutzgruppe (Vorgängergremium des EDSA) zum Thema der Anwendung und Festsetzung von Geldbussen (WP 253) weitergeführt. Ausserdem wurde die Überarbeitung des zentralen Bussgeldregisters des EDSA abgeschlossen und über Methoden zur Bestimmung «geringfügiger Verletzungen» diskutiert. Auch haben sich die Mitglieder der Arbeitsgruppe über wichtige nationale Bussgeld-Entscheidungen sowie relevante Gerichtsurteile ausgetauscht. Schliesslich wurde die temporäre Task Force Ende 2025 in eine ständige Arbeitsgruppe (Expertengruppe) des EDSA umgewandelt und ihre Zuständigkeit auf die Erarbeitung von Leitlinien zu sämtlichen Sanktionen der Datenschutz-Aufsichtsbehörden gemäss Art. 58 Abs. 2 DSGVO ausgeweitet *(Corrective Powers Expert Subgroup)*.

Diejenige Arbeitsgruppe des EDSA, welche sich mit der möglichst einheitlichen Durchsetzung der Bestimmungen der DSGVO in den Mitgliedstaaten befasst *(Enforcement Subgroup)*, war im Berichtsjahr mit der Weiterführung der Arbeiten an Leitlinien zu Art. 66 DSGVO und einer Mustervorlage für einen «massgeblichen und begründeten Einspruch» gemäss Art. 4 Ziff. 24 DSGVO beschäftigt. Zudem wurde die Arbeitsgruppe zur Behördenkooperation bei der Umsetzungsvorbereitung der neuen Verordnung zur Festlegung weiterer Verfahrensregeln für die Durchsetzung der DSGVO unterstützt. Im Rahmen des Projekts der strategischen Fälle konnte die gemeinsame Untersuchung mehrerer Aufsichtsbehörden zu Smart TVs abgeschlossen werden. An dieser Untersuchung hatte sich auch die DSS mit technischer Expertise beteiligt. Daneben hat die Arbeitsgruppe ein Pilotprojekt für ein über alle Behörden einheitliches europäisches Reporting zu ihrer Tätigkeit abgeschlossen. Die Erkenntnisse des Pilotprojekts fliessen in die weitere Ausarbeitung der künftigen, standardisierten Berichterstattung ein.

Wertvoll aus Sicht der DSS war darüber hinaus auch 2025 wieder der im Rahmen der Arbeitsgruppe regelmässig geführte Austausch über grössere laufende Verfahren oder wichtige Entscheidungen der Datenschutz-Aufsichtsbehörden in ihren jeweiligen Ländern. Speziell wurde im Berichtsjahr ausserdem über Verfahren und Entscheidungen in Zusammenhang mit Betroffenenrechten in Fällen der gesetzlichen Vertretung vulnerabler Personen und bei der Rechtsdurchsetzung gegenüber internationalen Unternehmen sowie über die Arbeit und Kompetenzen der Behörden im KI-Bereich gesprochen.

Die Arbeitsgruppe hat vor einigen Jahren auch das *Coordinated Enforcement Framework* ins Leben gerufen, im Rahmen dessen jedes Jahr von europäischen Datenschutz-Aufsichtsbehörden gemeinsam ein bestimmtes datenschutzrechtliches Thema europaweit untersucht wird. Ziel ist die weitere Harmonisierung der Rechtsauslegung und -anwendung durch die Aufsichtsbehörden. Als Mittel kommen dabei sowohl länderübergreifende Informationsbeschaffungen zur Eruierung des Status quo (für die Planung allfälliger weiterer Massnahmen) als auch gemeinsam lancierte, europaweite Kontrollen in Betracht. Jede Aufsichtsbehörde ist dabei frei zu entscheiden, ob sie sich an einer solchen koordinierten Aktion beteiligen will und welches Mittel sie einsetzen möchte.

Im Berichtsjahr wurde eine solche *Coordinated Action* zum Recht auf Löschung gemäss Art. 17 DSGVO durchgeführt. Die DSS hat sich daran beteiligt und mittels eines umfangreichen Fragebogens an fünf grosse Organisationen verschiedener Sektoren und Branchen in Liechtenstein Informationen darüber erhoben, wie dieses Betroffenenrecht in den Organisationen konkret umgesetzt wird. Die Antworten hat die DSS in einem nationalen Bericht zusammengefasst und die wichtigsten Erkenntnisse daraus sowie konkrete Handlungsempfehlungen den betrieblichen Datenschutzbeauftragten in Liechtenstein an ihrem jährlichen Vernetzungstreffen präsentiert. Der über alle teilnehmenden Länder aggregierte Abschlussbericht des EDSA wird auf europäischer Ebene anfangs 2026 veröffentlicht. Durch die im Rahmen solch koordinierter Aktionen gewonnenen Erkenntnisse kann die DSS die Organisationen in Liechtenstein noch besser unterstützen, indem sie zielgerichtete Weiterbildungen, Informationen und Beratung anbieten kann.

Für 2026 wurde bereits wieder eine neue Coordinated Action lanciert, welche sich mit Einhaltung der Transparenz- und Informationspflichten gemäss Art. 12, 13 und 14 DSGVO befasst. Obwohl eine aktive Beteiligung der DSS an dieser Aktion aus Ressourcengründen nicht vorgesehen ist, verfolgt sie die Entwick-

lungen aufmerksam und nutzt die auf europäischer Ebene gewonnenen Ergebnisse und Empfehlungen gezielt für die nationale Praxis.

Die bereits 2024 von der Arbeitsgruppe gegründete Task Force zur Anwendung von ChatGPT (ChatGPT Taskforce), welche die Zusammenarbeit und den Informationsaustausch zwischen den Aufsichtsbehörden bei Untersuchungen und Verfahren in Zusammenhang mit ChatGPT/OpenAI bezweckte, wurde im Berichtsjahr ebenfalls leicht angepasst. Sie befasst sich nun auch mit anderen Modellen generativer KI und stellt einen regelmässigen Austausch der Datenschutz-Aufsichtsbehörden sicher, insbesondere um deren jeweilige Verfahren gegen entsprechende Anbieter aus Drittstaaten besser koordinieren zu können *(Generative AI Enforcement Taskforce)*.

Von der Arbeitsgruppe, die sich mit der Zusammenarbeit der Aufsichtsbehörden befasst *(Cooperation Subgroup)*, wurde im Berichtsjahr erneut speziell das Verordnungsprojekt der EU-Kommission zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO eng begleitet, welches für eine europaweite Harmonisierung grenzüberschreitender Verfahren sorgen soll. So konnte aufgrund des finalen Gesetzestextes eine Analyse durchgeführt werden, welche Prozesse und Instrumente auf europäischer Ebene angepasst und welche Leitlinien des EDSA überarbeitet werden müssen. Mit den entsprechenden Anpassungsarbeiten wurde ebenfalls bereits begonnen, da die Verordnung schon im Herbst 2026 in Kraft treten wird. Daneben konnte auch die Überarbeitung der internen Leitlinien bzw. die Ausarbeitung von Best Practices zu Art. 64 Abs. 2 DSGVO bezüglich Stellungnahmen des EDSA im Berichtsjahr abgeschlossen werden. Zudem hat die Arbeitsgruppe die Überarbeitung der Leitlinien zu Art. 61 DSGVO zur gegenseitigen Amtshilfe sowie zu Art. 62 DSGVO zu gemeinsamen Massnahmen der Aufsichtsbehörden weitergeführt. Ebenso konnte an einem gemeinsamen europäischen Register der Vertreter von Organisationen aus Drittstaaten gemäss Art. 27 DSGVO weitergearbeitet werden. Schliesslich haben sich die Mitglieder auch im Berichtsjahr wieder über diverse kleinere Fragen bezüglich ihrer Zusammenarbeit ausgetauscht.

Die thematische Arbeitsgruppe zu Finanzangelegenheiten *(Financial Matters Subgroup)* hat auch im Berichtsjahr wieder das voranschreitende Projekt zur Einführung eines Digitalen Euros eng verfolgt und einen entsprechenden Austausch mit der Europäischen Zentralbank weitergeführt. Zudem erfolgte ein Austausch mit der Europäischen Bankenaufsichtsbehörde zu datenschutzrechtlichen Themen bei der Bekämpfung von Geldwäscherei und Terrorismusfinanzierung (AML/CFT) durch die neu dafür geschaffene europäische Behörde AMLA. Daneben wurde auch die eigene Arbeit zum Datenschutz bei AML/CFT-Massnahmen fortgesetzt, vorerst insbesondere zur Nutzung so genannter Watch Lists durch regulierte Finanzintermediäre. Und es wurde über Art. 75 der neuen europäischen Geldwäschereiverordnung diskutiert, welcher Partnerschaften der regulierten Finanzintermediäre zum entsprechenden Informationsaustausch ermöglicht. Darüber hinaus hat die Arbeitsgruppe im Berichtsjahr Empfehlungen zur Rechtsgrundlage bei der zwingenden Nutzerkontoeröffnung in Online-Shops erarbeitet und kleinere Beiträge und Stellungnahmen erarbeitet zu Themen wie FATCA, grenzüberschreitender Zahlungsverkehr oder Blockchain Technologien. Viele dieser Arbeiten werden auch 2026 fortgeführt.

Die neu geschaffene ständige Arbeitsgruppe des EDSA zu regulierungsübergreifenden Fragestellungen und dem Zusammenspiel von Wettbewerbs- und Datenschutzrecht *(Cross-Regulatory Interplay Expert Subgroup)* hat sich im Berichtsjahr insbesondere mit der Erarbeitung von gemeinsamen Leitlinien mit der Kommission zum Zusammenspiel des Gesetzes über digitale Märkte (DMA) und der DSGVO befasst. Ebenso hat sie Stellungnahmen zu Berichterstattungen im Rahmen des DMA vorbereitet und den EDSA in einigen Gremien des DMA vertreten. Darüber hinaus hat die Arbeitsgruppe eine Auslegeordnung zu den zusätzlichen Kompetenzen und Aufgaben der Datenschutz-Aufsichtsbehörden in Zusammenhang mit den diversen neuen europäischen Digital-Gesetzen erstellt, die Arbeit an einer Mustervorlage für eine Vereinbarung zur regulierungsübergreifenden Behördenzusammenarbeit sowie entsprechenden Good Practises aufgenommen und die Arbeitsgruppe für technologische Themen bei der Erarbeitung von Leitlinien zum Zusammenspiel von KI-Verordnung und DSGVO unterstützt. Begleitet wurde dies von weiteren punktuellen Diskussionen zu einschlägigen Themen im Rahmen des Mandats der Arbeitsgruppe.

Die Arbeitsgruppe zu Datenübermittlungen in Drittstaaten *(International Transfer Subgroup)* hat im Berichtsjahr ihre Arbeiten zu diversen Themen aufgenommen oder fortgesetzt. Die im Vorjahr erwähnte Arbeit an den Empfehlungen für verbindliche interne Datenschutzvorschriften für Auftragsdatenverarbeiter («Processor BCR») wurde im Berichtsjahr abgeschlossen. Wie schon im Vorjahr beschäftigte sich die Arbeitsgruppe im Berichtsjahr erneut mit den internen BCR-Genehmigungsverfahren beim EDSA. Hier besteht angesichts der hohen Arbeitsbelastung für die Aufsichtsbehörden sowie einzelner Verfahrensunstimmigkeiten weiterhin Optimierungspotenzial.

Die Arbeitsgruppe befasste sich zudem mit Fragen in Zusammenhang mit den jährlichen Aktualisierungen sowie der Durchsetzung der BCR. Diese Themen werden sie wohl auch in den kommenden Jahren begleiten. Zudem befasste sich die Arbeitsgruppe mit den Angemessenheitsbeschlüssen der Kommission für diverse Länder (Vereinigtes Königreich, Israel, Südkorea, Brasilien, Kenia und Japan) wie auch eine internationale Organisation (Europäisches Patentamt) und stand hierzu im Austausch mit der EU-Kommission, erarbeitete Stellungnahmen und tauschte sich mit anderen Arbeitsgruppen aus.

Die Compliance, E-Government und Health Subgroup (CEH-Arbeitsgruppe, *CEH Expert Subgroup*) befasst sich mit Zertifizierungen und Akkreditierungen sowie E-Government und Gesundheit. Betreffend Zertifizierung und Akkreditierung prüfte die CEH-Arbeitsgruppe die Akkreditierungskriterien für Zertifizierungsstellen nach Art. 43 DSGVO einzelner Mitgliedstaaten, zu denen der EDSA in der Folge eine Stellungnahme abgab. Ebenfalls war die CEH-Arbeitsgruppe mit einer Reihe ihr unterbreiteter Zertifizierungskriterien und Verhaltensregeln befasst, hinsichtlich welcher der EDSA in der Folge ebenfalls eine Stellungnahme nach Art. 64 DSGVO abgab. Die der Arbeitsgruppe im Berichtsjahr unterbreiteten und von ihr geprüften Zertifizierungskriterien sowie Verhaltensregeln umfassten die transnationalen Verhaltensregeln für die European Federation of Pharmaceutical Industries and Associations (Europäischer Verband der pharmazeutischen Industrie und Verbände, EFPIA), des Weiteren die Zertifizierungskriterien von Europrivacy, die Zertifizierungskriterien von Lexing, die Zertifizierungskriterein von For Humanity sowie den Kriterienkatalog der TÜV NORD CERT GmbH.

Im Bereich E-Government verfolgte die CEH-Arbeitsgruppe auch im Berichtsjahr erneut die massgebenden Entwicklungen bei den einschlägigen europäischen Digitalisierungsrechtsakten. Im Gesundheitsbereich schliesslich widmete sich die CEH-Arbeitsgruppe wieder insbesondere dem Entwurf der Leitlinien zur Verarbeitung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung. Auch im Berichtsjahr konnten dabei verschiedene offene Detailfragen analysiert und einer gemeinsamen Lösung zugeführt werden. Aufgrund der Komplexität der Materie dauert die Arbeit an den Leitlinien jedoch noch an. Schliesslich wurden gegen Ende des Berichtsjahres auch in der CEH-Arbeitsgruppe einschlägige Teile des von der EU-Kommission vorgelegten Digital Omnibus-Reformpakets diskutiert, da der EDSA gemeinsam mit dem EDSB eine Stellungnahme dazu ausarbeitete.

Die Arbeitsgruppe zu technologischen Themen *(Technology Expert Subgroup)* befasste sich im Jahr 2025 mit einem breiten Themenspektrum und arbeitete an mehreren Leitlinien, Empfehlungen und Stellungnahmen für den EDSA. So wurden unter anderem die Leitlinien zu Telemetrie und diagnostischen Daten, zum Zusammenspiel zwischen KI-Verordnung und DSGVO, zum Scraping von Daten zum Zweck des KI-Trainings, zur Anonymisierung und zur Pseudonymisierung sowie zur biometrischen Zugangskontrolle besprochen und bearbeitet. Während die Leitlinien zur Pseudonymisierung im Jahr 2025 vom EDSA verabschiedet und in die öffentliche Konsultation gegeben wurden, gestaltete sich die Erarbeitung der Leitlinien zur Anonymisierung weiterhin als äusserst herausfordernd und konnte noch nicht abgeschlossen werden. Die Leitlinien zur Pseudonymisierung befinden sich mittlerweile auf Grundlage der Ergebnisse der öffentlichen Konsultation in Überarbeitung. Eine entsprechende Veröffentlichung ist jedoch erst nach Abschluss auch der Anonymisierungsleitlinien geplant. Damit kann in Teilen voraussichtlich im ersten Halbjahr 2026 gerechnet werden.

Weitere Themen, die in der Arbeitsgruppe behandelt wurden, waren insbesondere die Vertretung des EDSA in einer Expertengruppe der EU-Kommission zum Zugang von Strafverfolgungsbehörden zu verschlüsselter Kommunikation, ein Vergleich der Sicherheit von Webshops mit und ohne Nutzerkonto sowie eine Vereinheitlichung der Meldeverfahren bei Datenpannen. Hinzu kamen die Initiierung einer Arbeitsgruppe, welche Vorlagen und Muster für eine gemeinsame Datenschutz-Folgenabschätzung (DSFA) erarbeitet sowie der Austausch mit anderen Behörden und weiteren Arbeitsgruppen des EDSA, um nur einige Beispiele zu nennen.

Im Jahr 2025 legte die Arbeitsgruppe für Soziale Medien *(Social Media Subgroup)* ihren Schwerpunkt auf die Ausarbeitung von Leitlinien zur Verarbeitung personenbezogener Daten zum Zwecke der Ausrichtung oder Bereitstellung politischer Werbung (auch als «Leitlinien zur Transparenz und Ausrichtung politischer Werbung» bezeichnet). Parallel dazu begann sie mit der Ausarbeitung vorbereitender Unterlagen für eine im Frühjahr 2026 geplante öffentliche Stakeholder-Veranstaltung betreffend das Thema dieser Leitlinien. Im September konnten zudem die Leitlinien zum Zusammenspiel zwischen dem Gesetz über digitale Dienste (Digital Services Act; DSA) und der DSGVO verabschiedet und in die öffentliche Konsultation gegeben werden. Die zahlreichen Rückmeldungen aus der Konsultationsphase werden in die entsprechende Überarbeitung der Leitlinien einfliessen. Die Veröffentlichung davon wird voraussichtlich für das erste Halbjahr 2026 erwartet.

Im Berichtsjahr setzte die DSS auch die Teilnahme an der BTLE-Arbeitsgruppe *(Border Travel and Law Enforcement Expert Subgroup)* fort, welche zentrale datenschutzrechtliche Entwicklungen in den Bereichen Polizei, Grenzverkehr und Strafjustiz koordiniert. Der inhaltliche Schwerpunkt der Arbeit lag 2025 erneut auf der Erarbeitung von Leitlinien zu den Rechten betroffener Personen nach der EU-Richtlinie 2016/680 (LED), insbesondere zum Recht auf Auskunft, sowie von Leitlinien zur Interaktion zwischen der KI-Verordnung und den EU-Datenschutzgesetzen (DSGVO und LED). Die Arbeiten erfolgten teilweise in Zusammenarbeit mit der Arbeitsgruppe zu technologischen Themen. Die Leitlinien zu Art. 48 DSGVO konnten nach Abschluss der öffentlichen Konsultation im Berichtsjahr finalisiert und veröffentlicht werden. Sie präzisieren die Voraussetzungen für internationale Datenübermittlungen auf Grundlage von Urteilen oder Entscheidungen von Behörden eines Drittstaats.

Ein weiterer Schwerpunkt der Arbeit lag auf Angemessenheitsentscheidungen der EU-Kommission gemäss Art. 45 DSGVO bzw. Art. 36 LED und deren Überprüfungen. Die Arbeitsgruppe wirkte in Zusammenarbeit mit der Arbeitsgruppe zu Datenübermittlungen an Drittstaaten an mehreren entsprechenden Stellungnahmen des EDSA mit, namentlich betreffend die Europäischen Patentorganisation, das Vereinigten Königreich sowie Brasilien. Zudem befasste sich die Arbeitsgruppe mit der ersten Überprüfung des Angemessenheitsbeschlusses für Südkorea, wobei die entsprechenden Arbeiten im Berichtsjahr noch nicht abgeschlossen werden konnten. Darüber hinaus wirkte die Arbeitsgruppe bei der Evaluierung der LED durch den EDSA gemäss Art. 62 LED mit.

Die Arbeitsgruppe KEYP *(Key Provisions Expert Subgroup)* befasst sich mit Schlüsselthemen der DSGVO und entwickelt dazu grundlegende Empfehlungen zur Auslegung und praktischen Anwendung der Datenschutzvorschriften. Diesen Arbeiten, oftmals auch in enger Zusammenarbeit mit anderen Expertengruppen vorgenommen, kommt eine besondere Bedeutung im Hinblick auf die einheitliche Rechtsanwendung der Datenschutzvorschriften zu. Im Berichtsjahr setzte die Arbeitsgruppe ihre Arbeiten an den Leitlinien zu Consent-or-Pay-Modellen fort. Zudem wurde die Arbeit an Leitlinien zur Verarbeitung personenbezogener Daten von Kindern weitergeführt, wobei insbesondere Fragen zur Altersverifikation und Altersabsicherung vertieft bearbeitet wurden. In diesem Zusammenhang verabschiedete der EDSA im Berichtsjahr auch eine von der Arbeitsgruppe vorbereitete Erklärung zur Altersfeststellung. Ferner wurde im Berichtsjahr eine gezielte Überarbeitung der Leitlinien für Datenschutzbeauftragte eingeleitet, nachdem der entsprechende Aktualisierungsbedarf festgestellt wurde. Zudem wurde die Überarbeitung der Leitlinien zum berechtigten Interesse nach Art. 6 Abs. 1 Bst. f DSGVO nach Abschluss der öffentlichen Konsultation gestartet. Darüber hinaus wurden auch andere Arbeitsgruppen in spezifischen Fragen unterstützt.

Ebenfalls beteiligt war die Arbeitsgruppe an der Ausarbeitung der gemeinsamen Stellungnahme des EDSA und des EDSB zum Vorschlag der EU-Kommission für eine Verordnung über Vereinfachungsmassnahmen für KMUs, insbesondere die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäss Art. 30 Abs. 5 DSGVO. Und schliesslich lag ein weiterer zentraler Arbeitsschwerpunkt der Arbeitsgruppe gegen Ende des Jahres auf der Vorbereitung der gemeinsamen Stellungnahmen von EDSA und EDSB zu den von der EU-Kommission vorgelegten AI-Omnibus und Digital Omnibus-Reformpaketen. Die Arbeitsgruppe hat in diesem Zusammenhang sowohl fachlich als auch koordinierend einen massgeblichen Beitrag geleistet.

Die Task Force zum internationalen Engagement der Mitglieder *(Taskforce on International Engagement)* fördert den Austausch unter den Datenschutz-Aufsichtsbehörden bezüglich ihrer Teilnahme und ihren Voten in multilateralen Foren zum Datenschutz und zum Schutz der Privatsphäre wie dem Europarat (Konvention 108), der Global Privacy Assembly (GPA), der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), dem G7 Data Protection Authorities Roundtable (G7 DPAR) oder der Spring Conference. Zu den Hauptaufgaben der Task Force zählen dabei die Koordinierung der EDSA-Beteiligung an internationalen Datenschutzveranstaltungen, der Informationsaustausch über globale Datenschutzentwicklungen sowie die Unterstützung einer einheitlichen europäischen Position in internationalen Debatten.

Im Berichtsjahr standen als zentrale Themen insbesondere die Vorbereitung des G7 DPAR, der Jahreskonferenz der GPA sowie der Spring Conference und die Abstimmung der Mitglieder hinsichtlich der Arbeiten der OECD zum Datenschutz im Fokus. Die Task Force tauschte sich dabei insbesondere zu aktuell bearbeiteten Themen und Entwicklungen in den genannten internationalen Foren aus, darunter Fragen der grenzüberschreitenden Durchsetzungszusammenarbeit, der Weiterentwicklung gemeinsamer Standards sowie thematische Schwerpunkte wie KI und Regulierung im Digitalbereich.

Das *DPO-Network* ist das Netzwerk der für die europäischen Datenschutz-Aufsichtsbehörden amtierenden Datenschutzbeauftragten. Ziel dieses Netzwerkes ist der Aufbau von gemeinsamem Know-how, der Erfah-

rungsaustausch unter den Datenschutzbeauftragten sowie die Erleichterung ihrer Arbeit durch Schaffung einheitlicher Standards. Zudem widmet sich das Netzwerk auch den ihm durch den EDSA zugewiesenen spezifischen Themen. Entsprechend der Zielsetzung des DPO-Netzwerkes befasste es sich auch im Berichtsjahr mit relevanten Fragestellungen und Themen in diesem Bereich. Aufgrund anderer prioritär zu behandelnden Agenden auf europäischer Ebene fanden 2025 keine Sitzungen statt. Allerdings war die Möglichkeit des Austauschs über das eingerichtete Forum stets möglich und die Zielsetzung auch damit erreicht.

7.1.3 Gegenseitige Amtshilfe

Die DSGVO erfordert neben der Zusammenarbeit der europäischen Datenschutz-Aufsichtsbehörden im bzw. mit dem EDSA auch eine intensive Kommunikation zwischen den einzelnen Aufsichtsbehörden, indem diese gemäss Art. 57 Abs. 1 Bst. g DSGVO «mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten». Die DSS erhielt im Berichtsjahr 212 Anfragen von anderen europäischen Datenschutz-Aufsichtsbehörden, was im Vergleich zu den im Vorjahr erhaltenen 162 Anfragen eine starke Zunahme um rund 24 % bedeutete. Die Anfragen wurden jeweils gestellt, wenn im Vollzug der aufsichtsrechtlichen Tätigkeit Interpretationsspielraum bestand und die anfragende Datenschutz-Aufsichtsbehörde die Rechtsmeinung anderer Aufsichtsbehörden bzw. die Anwendung von Bestimmungen der DSGVO durch andere Mitgliedstaaten erfahren wollte. Die Anfragen betrafen unter anderem folgende Themen: Auskunftsrecht, Biometrische Daten und Identifikation bei Zahlungsservices von Banken, Deepfake, Digital Identity Wallet, Einsatz von KI zur Planung medizinischer Kontrollen für krankgeschriebene Arbeitnehmer, Bekämpfung von Geldwäsche und Terrorismus-Finanzierung, KI und Algorithmen, KI-Kameras zur Altersüberprüfung bzw. -erkennung, Smart Doorbell und Domestic CCTV System, Microsoft Education 365, Phishing E-Mails, Recht auf Berichtigung, Richtlinien zu öffentlichem Zugang zu Grundbuchinformationen, Direct Marketing, Verarbeitung von personenbezogenen Daten für wissenschaftliche Forschungszwecke oder Videoüberwachung auf Privatgrundstücken.

Auch in diesem Jahr stellte die DSS fest, dass die Amtshilfeersuchen, dem allgemeinen Trend entsprechend, vermehrt komplexe datenschutzrechtliche Fragestellungen im Zusammenhang mit neuen Technologien betreffen. Ausserdem beziehen sich einige der gestellten Fragen auf Systeme und Technologien, die in Liechtenstein (noch) nicht zum Einsatz kommen. Dies stellt eine besondere Herausforderung dar, da es zunehmend schwieriger wird, alle diese Amtshilfeersuchen fundiert und praxisnah zu beantworten. Infolgedessen muss die DSS priorisieren, welche Anfragen sie vertieft bearbeiten kann und wo eine Beantwortung mangels praktischer Relevanz oder fehlender Erfahrungswerte nicht möglich ist.

7.2 Gemeinsame Massnahmen der Aufsichtsbehörden gemäss Art. 62 DSGVO

Der EDSA beschloss im Jahr 2022, eine länderübergreifende strategische Untersuchung zum Thema «Smart TV» zu starten. Da solche Geräte auch in Liechtenstein weit verbreitet sind, sagte die DSS ihre aktive Teilnahme zu und unterstützte die Untersuchung insbesondere mit technischer Expertise. Die länderübergreifende strategische Untersuchung zum Thema Smart TV konnte nun 2025 mit einem detaillierten Bericht abgeschlossen werden. Dieser stellt in der Folge die gemeinsame Basis für Verfahren der Datenschutz-Aufsichtsbehörden gegen einzelne Verantwortliche in diesem Bereich dar.

7.3 Schengen-Arbeitsgruppen

Die DSS engagiert sich aktiv in der europäischen Zusammenarbeit im Rahmen des Schengen-Acquis und nimmt regelmässig an den Sitzungen des **Coordinated Supervision Committee (CSC)** teil. Dieses Gremium setzt sich aus Vertreterinnen und Vertretern der nationalen Datenschutz-Aufsichtsbehörden sowie dem EDSB zusammen und gewährleistet eine koordinierte datenschutzrechtliche Aufsicht über IT-Grosssysteme sowie Einrichtungen, Ämter und Agenturen der EU gemäss Art. 62 der Verordnung (EU) 2018/1725 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union und zum freien Datenverkehr. Im Berichtsjahr fanden vier Sitzungen des CSC statt. Die koordinierte Aufsicht dieses Gremiums erstreckt sich bereits auf acht zentrale IT-Grosssysteme der EU, darunter das Schengen Information System (SIS), das Internal Market Information System (IMI), das Visa Information System (VIS), das Entry/Exit System (EES) sowie das European Travel Information and Authorisation System (ETIAS). Hervorzuheben ist, dass das EES im Berichtsjahr in Betrieb genommen wurde.

Obwohl ETIAS erst Ende 2026 in Betrieb gehen wird, wurden bereits im Berichtsjahr anspruchsvolle, weitreichende und komplexe Fragestellungen an die zuständige Arbeitsgruppe des CSC herangetragen. Die entsprechenden Diskussionen werden voraussichtlich bis ins Folgejahr andauern. Im Zentrum steht dabei die

Auslegung von Art. 4 Ziff. 9 DSGVO, insbesondere der dort vorgesehenen Ausnahme, wonach Behörden unter bestimmten Umständen nicht als Empfänger von personenbezogenen Daten zu klassifizieren sind. Wann und unter welchen Umständen dies der Fall sein kann, ist Gegenstand der gegenwärtigen Diskussion. Sollten etwa Strafverfolgungsbehörden im Rahmen von Zugriffen auf das ETIAS-System oder im Rahmen sogenannter «particular inquiries» nicht als Empfänger gelten, hätte dies unmittelbare Auswirkungen auf die Rechte der betroffenen Personen. So müssten diese im Rahmen von Auskunftsbegehren beispielsweise nicht mehr über die Weitergabe ihrer personenbezogenen Daten an entsprechende Behörden informiert werden. Daneben entstand auch eine Diskussion über die Abgrenzung der Anwendbarkeit der DSGVO und der LED. Gegen Ende des Berichtsjahres wurde zudem ein Mitarbeiter der DSS zum Koordinator der Arbeitsgruppe ernannt.

Im Berichtsjahr wurde bekannt, dass künftig noch weitere Systeme in den Aufgaben- und Aufsichtsbereich des CSC aufgenommen werden sollen. Dazu zählen unter anderem das Carbon Border Adjustment Mechanism Transitional Registry, das Information System on Deforestation and Forest Degradation sowie die European Asylum Dactyloscopy Database (EURODAC). Ausserdem sollen Aufsichtsfunktionen im Rahmen von Prüm II, der Interoperabilitätsarchitektur und des Data Act hinzukommen. Der Ausblick auf diese Ausweitung des Aufgabenbereichs, die auf den ersten Blick teilweise nur geringe inhaltliche Berührungspunkte mit den bislang beaufsichtigten Systemen erkennen lässt, führte zu intensiven Diskussionen innerhalb des Gremiums. Die Erweiterung wird damit begründet, dass in sämtlichen genannten Fällen eine Verarbeitung personenbezogener Daten stattfindet und die Systeme zudem von der europäischen Behörde EU-LISA gehostet werden. Es handle sich folglich um Konstellationen im Sinne von Art. 62 der Verordnung (EU) 2018/1725, womit die koordinierte Aufsicht durch das CSC eröffnet ist.

Weitere Themen und Fragestellungen, mit denen sich das CSC im Berichtsjahr befasste, betrafen beispielsweise die Frage, wie das gesetzlich vorgeschriebene Überprüfungsintervall für SIS genau zu interpretieren ist. Auch stellte sich die Frage, wie Log-Überprüfungen auszusehen haben bzw. was diese mindestens umfassen müssen. Da das EES im Berichtsjahr in Betrieb ging, begann das Gremium ausserdem mit der Ausarbeitung eines «Guide on Data Subject Rights» zu diesem System.

Die bereits erwähnte **EURODAC** ist ein zentrales IT-System der EU zur Unterstützung des Dublin-Systems im Asylwesen. Es ermöglicht mittels Fingerabdruckabgleich die Feststellung, welcher Mitgliedstaat für die Prüfung eines Asylantrags zuständig ist, indem überprüft wird, ob eine Person bereits in einem anderen Mitgliedstaat ein Asylgesuch gestellt hat. Seit 2013 können unter bestimmten Voraussetzungen auch Strafverfolgungsbehörden zum Zweck der Verhütung und Verfolgung schwerer Straftaten auf die Daten zugreifen. Zur Aufsicht über dieses System wurde bis zum Ende des Berichtsjahres ein **gemeinsames koordiniertes Aufsichtsgremium** geführt. Dieses hielt im Berichtsjahr zwei Sitzungen ab. Die Sitzung vom Dezember war jedoch die letzte in der bisherigen Form, denn mit Inkrafttreten der neuen gesetzlichen Bestimmungen bezüglich EURODAC wird die gemeinsame koordinierte Aufsicht in das CSC überführt.

7.4 Europarat

Die DSS hat im Berichtsjahr an der 48. und 49. Versammlung des Beratenden Ausschusses des **Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108)** des Europarats in Strassburg teilgenommen.

Der Beratende Ausschuss der Konvention 108 hat im Berichtsjahr weiter an Leitlinien zum Datenschutz im Bereich der Neurowissenschaften gearbeitet sowie die Arbeit an Leitlinien zum Datenschutz im Kontext von Large Language Models (LLMs) aufgenommen. Im Übrigen bestand die Hauptarbeit des Beratenden Ausschusses an der Erarbeitung von Berichten, Positionspapieren u.ä. Auch die Diskussion über geeignete Instrumente für grenzüberschreitende Datentransfers wurde fortgeführt. Die Ergebnisse all dieser Arbeiten können zu künftigen Handlungsempfehlungen, Leitlinien, Resolutionen oder Erklärungen auch übergeordneter Organe des Europarates führen.

Vor Kurzem wurde die Konvention 108 mittels eines Änderungsprotokolls modernisiert und insbesondere an die heutigen informations- und kommunikationstechnologischen Möglichkeiten der Datenverarbeitung angepasst. Einschliesslich Liechtenstein haben bereits 33 Staaten das Änderungsprotokoll ratifiziert. Damit fehlen nur noch 5 Ratifizierungen bis zum Inkrafttreten des Änderungsprotokolls bzw. der modernisierten Konvention 108+, was in naher Zukunft erwartet wird. Der Beratende Ausschuss hat sich entsprechend im Berichtsjahr auch mit dem angestrebten Inkrafttreten des Änderungsprotokolls befasst sowie Leitlinien zur Auslegung von Art. 11 der modernisierten Konvention 108+, welcher verschiedene Ausnahmen regelt, verabschiedet.

«Auf europäischer Ebene bleibt die Herstellung eines tragfähigen Gleichgewichts zwischen technologischem Fortschritt und dem Schutz der Privatsphäre zentral.»

8. Schlussbemerkung und Ausblick

Auch im Jahr 2026 wird sich die digitale Welt mit unverminderter Dynamik weiterentwickeln. Auf europäischer Ebene bleibt die Herstellung eines tragfähigen Gleichgewichts zwischen technologischem Fortschritt und dem Schutz der Privatsphäre zentral – sei es durch neue Rechtsakte oder durch die Weiterentwicklung bestehender Regelwerke.

Junge Menschen kommen dabei immer früher mit KI, sozialen Netzwerken und digitalen Anwendungen in Kontakt. Ein reflektierter Umgang mit KI-Systemen und personenbezogenen Daten wird zwar zunehmend im schulischen Kontext vermittelt; faktisch beginnt die digitale Sozialisation jedoch häufig deutlich früher – etwa durch elterliche Nutzung digitaler Dienste oder interaktive, vernetzte Spielzeuge.

Vor diesem Hintergrund wird die DSS im Jahr 2026 einen besonderen Schwerpunkt auf den Datenschutz von Kindern und Jugendlichen sowie auf die Förderung eines sicheren und verantwortungsvollen Umgangs mit Technologien legen. Die Informationsangebote auf der Internetseite sollen weiter zielgruppenspezifisch ausgebaut, sprachlich vereinfacht und didaktisch angepasst werden. Ziel ist es, Minderjährige frühzeitig zur Wahrnehmung ihrer Rechte zu befähigen und zugleich Erziehungsberechtigte sowie Bildungseinrichtungen mit praxisnahen Leitlinien zu unterstützen. Die Abwägung zwischen den Risiken komplexer datenintensiver Anwendungen und deren gesellschaftlichem sowie pädagogischem Nutzen bleibt dabei eine zentrale Herausforderung.

Eine weitere Entwicklung, die die behördliche Praxis zunehmend prägt, ist die verstärkte Nutzung generativer KI-Systeme – etwa ChatGPT und vergleichbarer Anwendungen – durch Beschwerdeführer und Beschwerdegegner. Eingaben werden vermehrt automatisiert erstellt und weisen nicht selten sachliche Fehler, unzutreffende Rechtszitate oder verkürzte Argumentationsketten auf. Dies führt dazu, dass ein erheblicher Teil der Verfahrensarbeit der DSS in der Identifikation und Korrektur inhaltlicher Unrichtigkeiten besteht, bevor eine materielle datenschutzrechtliche Prüfung erfolgen kann.

Gleichzeitig stehen der DSS weiterhin nur begrenzte personelle Ressourcen zur Verfügung. Angesichts steigender Fallzahlen, zunehmender technischer Komplexität und zusätzlicher Aufgaben ist eine konsequente Priorisierung erforderlich. Die Sicherstellung einer qualitativ hochwertigen, fundierten und zeitgerechten Aufgabenerfüllung bleibt daher auch im Jahr 2026 einmal mehr eine grosse Herausforderung.

Datenschutzstelle Fürstentum Liechtenstein
Kirchstrasse 8
Postfach 684
FL-9490 Vaduz
Telefon +423 236 60 90
info.dss@llv.li
www.datenschutzstelle.li