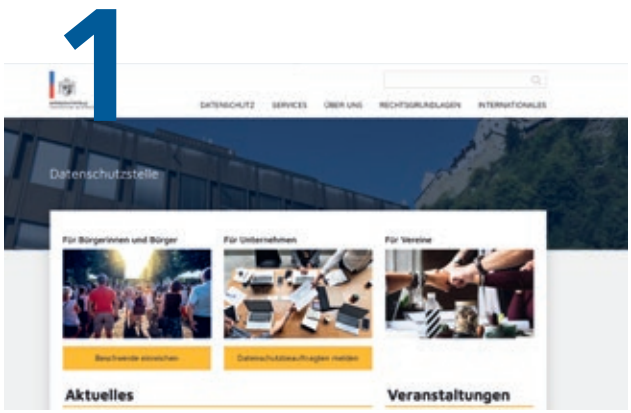
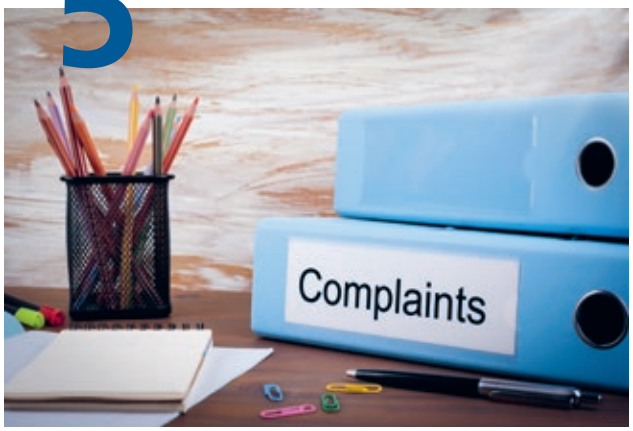
DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht Datenschutzstelle
Fürstentum Liechtenstein

Tätigkeitsbericht 2024

Inhaltsverzeichnis





Impressum

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

Vorwort

Das Jahr 2024 hielt für die DSS nicht nur herausfordernde Datenschutzfragen, sondern auch einen kleinen Moment des Schmunzelns bereit. Zwei Anfragen und ein Eintrag auf einer Internetseite bezogen sich auf die «Datenschutz-Grundversorgung» – ein Begriff, der so gar nicht in die Datenschutz-Grundverordnung (DSGVO) passt. Ob es sich dabei um einen Tippfehler, eine kreative Wortschöpfung oder einfach die Laune einer automatischen Rechtschreibkorrektur handelte, bleibt offen. Doch so amüsant dieser Lapsus auch war, er regt durchaus zum Nachdenken an: Ist Datenschutz nicht tatsächlich eine Form der Grundversorgung für unsere digitale Gesellschaft?

Denn eine Datenschutz-Aufsichtsbehörde, die seit nunmehr sieben Jahren die wirksame Durchsetzung des Datenschutzrechts verfolgt, sollte genau daran gemessen werden. Eine effektive «Datenschutz-Grundversorgung» bedeutet, für Bürgerinnen und Bürger sowie Unternehmen und öffentliche Stellen offen zugänglich zu sein, kleine wie grosse Anliegen ernst zu nehmen, erfolgreich gegen rechtswidrige Datenverarbeitungen vorzugehen und stets am Puls der technologischen und rechtlichen Entwicklungen zu bleiben.

Diese Grundversorgung sollte insbesondere dann nicht aus den Augen verloren werden, wenn Künstliche Intelligenz (KI) immer stärker in unseren Alltag einzieht. Während sie als grosse technologische Errungenschaft gefeiert wird, besteht die Gefahr, dass sie die grundlegenden Aspekte des Datenschutzes und der Privatsphäre in den Hintergrund drängt. Doch gerade angesichts dieser Neuerungen ist es essenziell, die Grundversorgung nicht zu vernachlässigen, denn sie ist es, die uns auch in Zeiten technologischer Umbrüche ermöglicht, die Privatsphäre weiterhin zu bewahren – unabhängig davon, welche Innovationen auf uns zukommen. Dabei darf nicht ausser Acht gelassen werden, dass Datenschutz nicht nur eine rechtliche Notwendigkeit, sondern auch eine gesellschaftliche Verantwortung ist. In einer Zeit, in der Daten immer mehr zur Währung werden und digitale Geschäftsmodelle zunehmend auf der Verarbeitung personenbezogener Informationen basieren, ist es umso wichtiger, dass Datenschutz nicht als Hindernis, sondern als Grundpfeiler einer modernen und vertrauenswürdigen digitalen Gesellschaft verstanden wird. Die Balance zwischen technologischer Innovation und dem Schutz der Privatsphäre ist daher eine der grössten Herausforderungen unserer Zeit – eine Herausforderung, der sich die DSS mit Entschlossenheit stellt.

Dr. Marie-Louise Gächter, Leiterin Datenschutzstelle

An dieser Stelle möchte ich meinen besonderen Dank an die Mitarbeitenden der DSS aussprechen. Sie tragen diesen Gedanken der Grundversorgung nicht nur mit, sondern setzen ihn mit grossem Engagement, Fingerspitzengefühl und Fachwissen um. Ihre Arbeit erfordert nicht nur rechtliches und technisches Know-how, sondern auch zwischenmenschliches Feingefühl, um in einem immer komplexer werdenden Datenschutzumfeld die richtigen Lösungen zu finden. Ohne ihren Einsatz wäre die DSS nicht das, was sie heute ist – eine zugängliche, kompetente und verlässliche Anlaufstelle für Datenschutz in Liechtenstein.

Der vorliegende Jahresbericht 2024 gibt Einblick in die vielseitige Arbeit der DSS, die stetig wachsenden Herausforderungen und die sich wandelnden Anforderungen an den Datenschutz. Er zeigt auf, wie wir unserer Aufgabe nachkommen, rechtliche Klarheit zu schaffen, Transparenz zu fördern und den Schutz personenbezogener Daten als unverzichtbaren Bestandteil einer digitalen Gesellschaft zu verankern. In diesem Sinne bleibt die DSS auch im kommenden Jahr bestrebt, eine verlässliche Instanz für alle Datenschutzfragen zu sein – vielleicht nicht als offizieller «Grundversorger», aber definitiv als unverzichtbarer Partner für einen starken und zukunftsfähigen Datenschutz.

Vaduz, im April 2025

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

1. Öffentlichkeitsarbeit

Die gesetzlich geforderte Vermittlung von Wissen im Bereich Datenschutz unterstreicht die entscheidende Rolle der Öffentlichkeitsarbeit für die Arbeit der DSS. Grundsätze und Neuerungen im Datenschutzrecht ebenso wie die datenschutzrechtlichen Standpunkte der Aufsichtsbehörde(n) sowie anderer relevanter Institutionen, wie des Europäischen Datenschutzausschusses (EDSA) oder nationaler und europäischer Gerichte, müssen einer breiten Öffentlichkeit bekannt gemacht und sowohl für Verantwortliche als auch für betroffene Personen leicht zugänglich gestaltet 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. Eine solche sich verbreitende, jedoch kritische Datenverarbeitung beobachtete die DSS im Berichtsjahr etwa im Bereich von Telefonaufzeichnungen. Auf Grund mehrerer Hinweise wurde bekannt, dass zahlreiche Institutionen Telefongespräche generell aufzeichnen, ohne dafür eine gesetzliche Verpflichtung zu haben oder die Einwilligung der betroffenen Personen eingeholt zu haben.

Ein neuer inhaltlicher Schwerpunkt der Wissensvermittlung lag in diesem Jahr zudem auf dem Thema Künstliche Intelligenz (KI), da hier aktuell ein besonders hoher Informationsbedarf festzustellen ist. Insbesondere wurden der Zusammenhang zwischen KI und Datenschutz sowie die Einhaltung der DSGVO im Kontext von KI-Anwendungen ausführlich behandelt.

Diese Erkenntnisse zeigen erneut deutlich auf, dass Datenschutz ohne eine aktive 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 18. Datenschutztag fand wie üblich zu Beginn des Jahres am 25. Januar im Gemeindesaal in Triesen statt. Mit dem Thema «Smart Home – Risiken und Nebenwirkungen» widmete sich die DSS Datenverarbeitungen rund um Wohnräume. Lichter über eine App dimmen, die Musik mit Sprachsteuerung ein- und ausschalten, Gesundheitsdaten auf dem Handy überwachen, Live-Überwachung und Aufzeichnung von Aktivitäten im und um das Haus oder Spielzeug, das mit Kindern interagiert; dies sind alles Elemente der faszinierenden Welt des Smart Homes. Nach der Begrüssung durch die Leiterin der DSS nahm Olivier Steiger, Professor an der Hochschule Luzern, die Besucher mit auf eine fesselnde Zeitreise durch die Entwicklung der Heimautomatisierung, in der er einen spannenden Einblick in die Vergangenheit, Gegenwart und Zukunft des vernetzten Wohnens gab. Darauf folgte eine praxisnahe Demonstration durch zwei Experten des Vereins Cybersecurity Liechtenstein. Sie informierten und veranschaulichten, wie über Schwachstellen auf Daten zugegriffen werden könnte. Nach einer Podiumsdiskussion, die von einem Bauherrn von Smart Homes durch interessante Einblicke und Anekdoten bereichert wurde, konnten diverse Fragestellungen bei einem anschliessenden Apéro weiter vertieft werden.

Am 11. November wurde das jährliche Vernetzungstreffen für Datenschutzbeauftragte im Kellertheater beim Vaduzer Saal abgehalten. Der Dialog mit den Datenschutzbeauftragten ist von zentraler Bedeutung für die Arbeit der DSS. In diesen Gesprächen kann festgestellt werden, wo Bedarf an zusätzlicher Aufklärung und Unterstützung besteht. Gleichzeitig legt die DSS grossen Wert darauf, den Datenschutzbeauftragten Einblicke in die Tätigkeit der Behörde zu ermöglichen. Dazu gehören insbesondere Informationen zu getroffenen Entscheidungen der DSS, Richtlinien und Entscheidungen des EDSA sowie wegweisenden Entscheidungen und Urteilen im In- und Ausland, die als Basis für Rechtssicherheit und als wertvolle Orientierungshilfen dienen. Dieser offene und transparente Austausch mit den Datenschutzbeauftragten stärkt die Zusammenarbeit und Effizienz im Bereich Datenschutz nachhaltig.

Wie bereits im Vorjahr vermittelte die DSS auch 2024 anlässlich des Vernetzungstreffens einen Überblick über die Ergebnisse einer weiteren vom EDSA organisierten und europaweit koordinierten Unter-

suchung zu einem bestimmten Thema, an der auch die DSS teilgenommen hatte. Im Rahmen dieser Untersuchung waren mittels eines umfangreichen Fragebogens an fünf grosse Organisationen verschiedener Sektoren und Branchen in Liechtenstein Informationen darüber erhoben worden, wie das datenschutzrechtliche Auskunftsrecht gemäss Art. 15 DSGVO in den befragten Organisationen genau umgesetzt wird. Die Antworten wurden von der DSS in einem nationalen Bericht zusammengefasst und die wichtigsten Erkenntnisse daraus, einschliesslich konkreter Handlungsempfehlungen, den betrieblichen Datenschutzbeauftragten an diesem Vernetzungstreffen präsentiert. Der über alle teilnehmenden Länder aggregierte Abschlussbericht zur Untersuchung des EDSA wird auf europäischer Ebene anfangs 2025 veröffentlicht werden. Mit den im Rahmen solcher koordinierter Aktionen gewonnenen Erkenntnissen kann die DSS die verschiedenen Organisationen in Liechtenstein und ihre jeweiligen Datenschutzbeauftragten künftig noch besser unterstützen, indem sie zielgerichtete Weiterbildungen, Informationen und Beratung anbieten kann.

Für 2025 wurde bereits wieder eine neue europaweite Untersuchung vom EDSA lanciert, welche sich mit der Umsetzung des Rechts auf Löschung gemäss Art. 17 DSGVO befassen wird. Auch daran wird die DSS teilnehmen.

Zwar konnte im Berichtsjahr selbst keine weitere Veranstaltung im Rahmen der Reihe «Datenschutz goes Cinema» mehr durchgeführt werden, doch laufen die Planungen für den nächsten Kino-Anlass der DSS bereits auf Hochtouren. Dieser wird im Verlaufe von 2025 stattfinden und voraussichtlich unter dem Thema «Identitätsdiebstahl» stehen. Im Rahmen dieser Veranstaltungsreihe zeigt die DSS jeweils einen Film im Kino und führt danach mit Experten eine Podiums-Diskussion zu einem datenschutzrechtlich relevanten Thema des Films durch. Das Veranstaltungsformat fand in der Bevölkerung jeweils grossen Anklang, weswegen es fortgesetzt wird.

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 14. November fand an der Privaten Universität im Fürstentum Liechtenstein (UFL) zum sechsten Mal eine ganztägige Weiterbildungsveranstaltung zum Thema «Datenschutz – Fachwissen für Expertinnen und Experten» statt. Diese Veranstaltungsreihe wird seit nunmehr sechs Jahren von der UFL in Zusammenarbeit mit der Datenschutzstelle, dem Datenschutzverein in Liechtenstein, der Liechtensteinischen Industrie- und Handelskammer, der BWB Rechtsanwälte AG, den Privacyofficers.at und der Data Privacy Community angeboten. Der Vortrag der DSS befasste sich mit dem Thema «Löschen unter der DSGVO: Offene Fragen und rechtliche Grauzonen». Das Recht auf Löschung, auch bekannt als das «Recht auf Vergessenwerden», zählt zu den zentralen Betroffenenrechten der DSGVO. Trotz der recht klaren gesetzlichen Regelungen bleiben in der Praxis zahlreiche Fragen offen. Der Vortrag der DSS beleuchtete aktuelle Herausforderungen und rechtliche Unsicherheiten rund um das Löschen von personenbezogenen Daten. Im Fokus standen vor allem die Abgrenzung zwischen Löschung und Anonymisierung, technische Umsetzbarkeit, Löschfristen sowie die Rechte betroffener Personen gegenüber Verantwortlichen und Auftragsverarbeitern. Darüber hinaus wurden die Grenzen dieses Rechts, etwa im Kontext der Archivierungspflichten, und die noch ungeklärten Fragen bei der Löschung in dezentralen Systemen und sozialen Netzwerken diskutiert. Ziel des Vortrags war es, einen Überblick über den aktuellen Stand der Diskussion zu geben und die bestehenden rechtlichen Grauzonen herauszustellen.

Darüber hinaus bot die DSS in Kooperation mit der UFL im Vorfeld des Fortbildungsseminars auch einen Intensivkurs zum 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 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.

Auf Einladung der Universität Liechtenstein übernahm die DSS im März des Berichtsjahres neun Lektionen im Rahmen des Zertifikatsstudiengangs «Digital Legal Officer». Ein erster Teil befasste sich mit den rechtlichen Fragen rund um die Umsetzung der Anforderungen der DSGVO in einem Unternehmen. Der zweite Teil widmete sich technischen As-

pekten und ging auf Detailfragen zu Datensicherheit, Datenschutz-Folgenabschätzung und der Meldung von Datenschutzverletzungen ein. Ebenso erfolgten Ausführungen zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie zu einem rechtskonformen Cookie Management.

1.2.2 «Behörden in Liechtenstein – Gemeinsam für Cyber-Sicherheit»

Am 13. November lud die DSS in Zusammenarbeit mit der Stabsstelle für Cyber-Sicherheit und der Landespolizei Unternehmen zur Veranstaltung «Behörden in Liechtenstein – Gemeinsam für Cyber-Sicherheit» ein. Ziel der Veranstaltung war es, den Teilnehmenden die Vorgehensweisen der Behörden sowie die Handlungsoptionen und Meldepflichten von Unternehmen im Falle eines Cyber-Sicherheitsvorfalls anschaulich zu vermitteln. Zudem wurden sowohl technische Analysemethoden als auch die internationale Kooperation und Vernetzung der Behörden thematisiert.

1.2.3 Tag der Menschenrechte zum Thema «KI und Menschenrechte»

Anlässlich des Tags der Menschenrechte am 10. Dezember beteiligte sich die DSS am Abendprogramm des Vereins für Menschenrechte in Liechtenstein mit dem Schwerpunkt «KI und Menschenrechte». In einem Fachvortrag erläuterte die DSS, welche Massnahmen und Verpflichtungen die aktuellen Regulierungen der KI im Rahmen der Europäischen Union und des Europarats vorsehen, um die Wahrung der Menschenrechte im Zusammenhang mit KI sicherzustellen.

1.2.4 Workshops an der Realschule Schaan

Am 18. Dezember führte die DSS im Rahmen eines Thementages zu Menschenrechten an der Realschule Schaan kurze Workshops durch. Die Schülerinnen und Schüler wurden dabei in kleine Gruppen eingeteilt und konnten im Laufe des Vormittags unterschiedliche Themen näher kennen lernen, darunter auch den Datenschutz. Die DSS führte dazu viermal jeweils 30-minütige Workshops durch. Dabei wurden mit den Kleingruppen interaktiv diverse datenschutzrechtlich relevante Fragen erörtert und diskutiert. Es ging vor allem darum, den Schülerinnen und Schülern einen ersten grundlegenden Einblick in juristische Fragestellungen wie auch den Anwendungsbereich des Datenschutzes zu geben.

1.2.5 Fachgruppe Medienkompetenz LIHGA 2024

Im Rahmen der Beteiligung der DSS bei der Fachgruppe Medienkompetenz war ein Schwerpunkt im Berichtsjahr die Teilnahme an der LIHGA unter dem Motto «Vorbilder». Um möglichst viele Personen zu begeistern, hatte die Fachgruppe vier Stationen eingerichtet, bei denen sich interessierte Besucher aktiv beteiligen konnten. Neben zwei Umfragen, einem Mitmach-Tanzvideo sowie zwei Bastelvideos für das jüngere Publikum, sorgten KI-generierte Plakate für interessante Diskussionen. Ziel der Fachgruppe war die Sensibilisierung der Bevölkerung zur eigenen Mediennutzung im Hinblick auf die Vorbildfunktion.

1.2.6 Schulungen für einzelne Berufsgruppen

Auf Anfrage eines Architektenbüros präsentierte die DSS die neuesten Entwicklungen im Datenschutzrecht, die von besonderem Interesse für diese Berufsgruppe sind. Einer weiteren Anfrage aus dem Treuhandbereich für eine entsprechende Schulung wird im Januar 2025 Folge geleistet.

1.2.7 Weitere Vorträge

Darüber hinaus engagierten sich die Mitarbeitenden der DSS bei über zehn weiteren Informations- und Diskussionsveranstaltungen. Sie hielten Fachvorträge, Vorlesungen und Schulungen – vor allem an der Universität Liechtenstein und der UFL, aber auch im Rahmen von Vereinsveranstaltungen und für den Privatsektor.

So hat die DSS auch im Berichtsjahr wieder an einer Fachveranstaltung in Zürich für betriebliche Datenschutzexperten aus der Schweiz teilgenommen. Hier präsentierte die DSS ihre Perspektiven zu aktuellen Entwicklungen im Datenschutz. Darüber hinaus war die DSS mit Vorträgen beim Privacy Ring in Luzern und in Wien und bei der Jahrestagung 2024 der Datenschutzbeauftragten der öffentlichen Verwaltung Österreichs in Linz vertreten.

Diese vielfältigen Aktivitäten unterstreichen die zentrale Rolle der DSS in der Datenschutzaufklärung und Wissensvermittlung. Sie demonstrieren das breite Engagement der Behörde, um sowohl die Öffentlichkeit als auch Fachkreise für die Herausforderungen und Entwicklungen im Bereich Datenschutz zu sensibilisieren.

1.3 Internetseite

Zwei weitere zentrale Säulen der Öffentlichkeitsarbeit der DSS sind der Internetauftritt und der im Berichtsjahr ca. monatlich versandte Newsletter. Diese beiden 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 erneut eine deutliche Zunahme der Zugriffe. Dies unterstreicht nicht nur die Relevanz der bereitgestellten Informationen, sondern auch die wachsende Nachfrage nach qualitativ hochwertigen Ressourcen im Bereich Datenschutz. Die verstärkte 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.

Rund drei Viertel aller Zugriffe auf die Rubrik «Datenschutz / Themen A–Z» der Internetseite wurden bei folgenden Beiträgen verzeichnet: Berechtigtes Interesse, besondere Datenkategorien nach Art. 9 und 10 DSGVO, Informationspflicht nach Art. 13 und 14 DSGVO, kleines Konzernprivileg sowie Profiling.

1.4 Newsletter

Ende 2024 hatten 1'079 Personen den Newsletter der DSS abonniert, was einem Plus von 13,6% gegenüber dem Vorjahr entspricht. Das Interesse am Newsletter ist somit nach wie vor ungebrochen. Im Berichtsjahr hat die DSS insgesamt 17 neue Informationsbeiträge und Veranstaltungsankündigungen auf ihrer Internetseite veröffentlicht und dazu 10 Newsletter versandt. Die drei meistgelesenen Newsletter 2024 waren: Google Street View in Liechtenstein, Aktuelles aus der Datenschutzstelle #2 sowie jener zur Europäischen Initiative zum Auskunftsrecht.

Sämtliche Newsletter können jederzeit auf der Internetseite der DSS nachgelesen werden. Ausserdem finden sich die meisten Inhalte der Newsletter dort 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 überprüfen zu müssen.

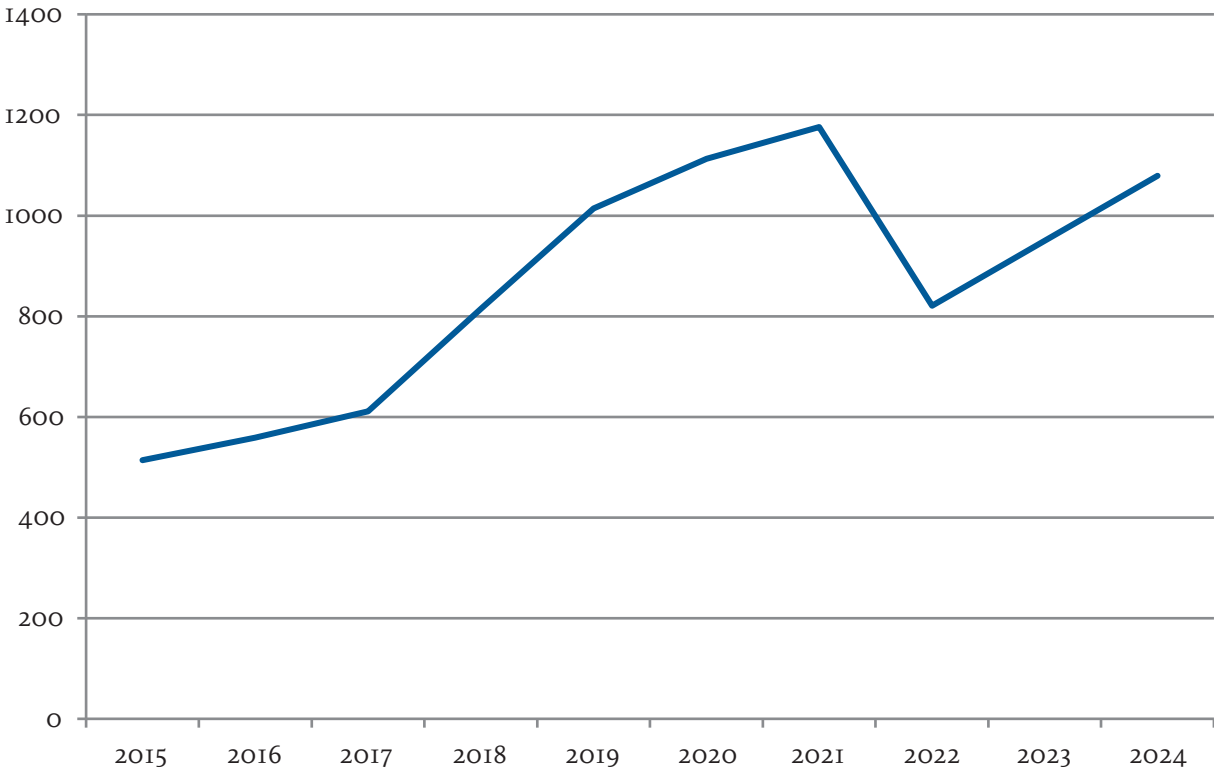


Abbildung 1: Entwicklung Newsletter-Abonnentinnen und Abonnenten

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 der Datenschutz wieder regelmässig in den liechtensteinischen Medien vertreten, wobei die Anzahl der Berichte mit knapp 30 Berichten leicht gegenüber dem Vorjahr anstieg. Die Themen in den Printmedien konzentrierten sich vor allem auf Fragen rund um das Thema KI, Google Street View, die Videoüberwachung am Weiherring, die eID für Unternehmen oder das Gesundheitsdossier.

Die mediale Berichterstattung zu datenschutzrechtlichen Themen und ihre positive Haltung gegenüber diesem Bereich leisten einen wertvollen Beitrag zur Umsetzung des kommunikativen Konzepts der DSS im Wissenstransfer. Dadurch werden auch Privatpersonen erreicht, die beruflich weniger mit Datenschutz in Berührung kommen, und erhalten einen verständlichen Zugang zu dieser Materie. Gleichzeitig zeigt die Berichterstattung, dass zunehmend Themen in den Fokus rücken, die über den klassischen Datenschutz hinausgehen und aktuelle Entwicklungen wie insbesondere das Potenzial Künstlicher Intelligenz in den Mittelpunkt stellen.

«Privatpersonen machten mit 20,3 % ein Fünftel der Fragestellenden aus und zeigten erneut ein starkes Interesse am Datenschutz»

2. Beratung zu konkreten Anfragen

2.1 Allgemeines

Im Berichtsjahr bearbeitete die DSS insgesamt 1'521 Anfragen von öffentlichen und privaten Institutionen sowie von Privatpersonen. Im Vergleich zu den 1'788 Anfragen des Vorjahres entspricht dies einem Rückgang um 15%. Über die letzten vier Jahre hinweg lässt sich jedoch ein klarer Trend zur steigenden Komplexität der Anfragen erkennen, der sich auch im Berichtsjahr fortsetzte.

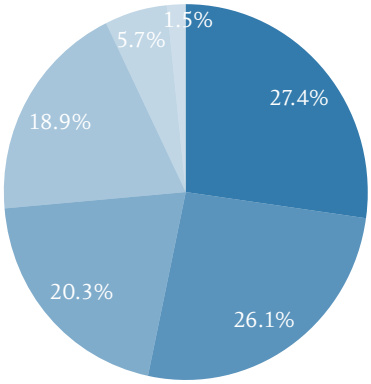
Die fortschreitende technologische Entwicklung führte zu einer Vielzahl neuer und anspruchsvoller Fragestellungen, insbesondere im Hinblick darauf, ob und wie technische Systeme die Anforderungen des Datenschutzes erfüllen können. Besonders der Einsatz von KI sorgte für zahlreiche Anfragen von Verantwortlichen. Ein weiterer Beratungsschwerpunkt lag auf der Nutzung von Videoüberwachungsanlagen durch private oder kommerzielle Akteure. Hinzu kamen Fragestellungen zu den sich abzeichnenden neuen Digitalisierungsrechtsakten der Europäischen Union, wie etwa dem Digital Services Act (DSA), dem Digital Markets Act (DMA) und dem Artificial Intelligence Act (AI Act oder KI Verordnung). Diese Regulierungen, die für den EWR-Staat Liechtenstein in unterschiedlichem Masse relevant sind, erfordern nicht nur eine Anpassung bestehender Systeme, sondern auch eine umfassende Aufklärung der Verantwortlichen über ihre Pflichten und die Einhaltung der DSGVO im Zusammenspiel mit diesen neuen EU-Vorschriften.

Die Herkunft der Anfragen zeigt ein vielfältiges Bild: Jeweils rund ein Viertel der Anfragen stammte aus dem öffentlichen Sektor (27,4%) sowie der Privatwirtschaft (26,1%). Der Grossteil der Anfragen aus dem privaten Sektor kam dabei von kleinen und mittleren Unternehmen verschiedener Branchen. An dritter Stelle folgten Privatpersonen, die mit 20,3% ein Fünftel der Fragestellenden ausmachten und erneut ein starkes Interesse am Datenschutz zeigten. Internationale Anfragen belegten mit 18,9% den vierten Platz. Anfragen von Vereinen und Stiftungen (5,7%) sowie von Medien (1,5%) gab es am wenigsten, doch nahmen sie im Berichtsjahr ebenfalls leicht zu.

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 welche zentrale Rolle der DSS bei der Unterstützung und Information der betroffenen Akteure zukommt.

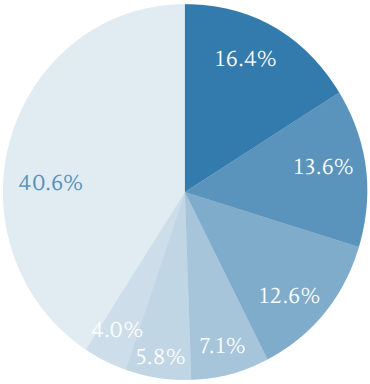
Beratungsanfragen konnten telefonisch, schriftlich – insbesondere mittels E-Mail – oder auch in einem persönlichen Gespräch bei der DSS eingebracht werden.

Wer stellt die Fragen?



- Behörden
- Privatwirtschaft
- Privatpersonen
- Internationales
- Vereine und Stiftungen
- Medien

Verteilung der Anfragen aus der Privatwirtschaft



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

Von den 1'521 Anfragen wurden im Berichtsjahr 159, also rund 10%, telefonisch gestellt und beantwortet. Sie stammten von 135 Anrufern, was einem Rückgang ungefähr auf das Niveau von 2022 entspricht (2023: 195 Anrufer; 2022: 144 Anrufer). Erklären lässt sich die nicht unbedeutende Zahl der telefonisch an die DSS gerichteten Anfragen damit, dass inzwischen zahlreiche Organisationen in regelmässigem Austausch mit der DSS stehen und somit über gute Kontakte zu deren Mitarbeitenden verfügen. In solchen Fällen ist ein Telefonat oftmals der schnellere Weg zur Lösung eines datenschutzrechtlichen Problems, da der Ansprechpartner bzw. die Ansprechpartnerin bei der DSS bereits einen guten Einblick in den datenschutzrechtlichen Alltag der anrufenden Person hat und weitere Fragen meist einfach und pragmatisch beantworten kann.

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 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» muss.

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 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.

Allerdings entschied die DSS bereits 2023, ihre Strategie zur Abgrenzung zwischen Untersuchung und Beratung insofern etwas anzupassen, als sie Beratungstermine für die Umsetzung einer rechtskräftigen Verfügung anbietet, wenn dies gewünscht wird.

2.2 Videoüberwachung und Veröffentlichung von Bildmaterial

Wie auch schon in den vergangenen Tätigkeitsberichten ausgeführt, ist und bleibt die Videoüberwachung ein stetiges Thema, mit dem sich die DSS zu beschäftigen hat. Wenngleich die Anwendungsbereiche grundsätzlich dieselben blieben, verzeichnete die DSS im Berichtsjahr eine Zunahme von Videoüberwachungen, die Baustellenfortschritte erfassen. Diese Videoüberwachungen unterscheiden sich von «klassischen» Überwachungen insofern, als sie keinem Sicherheitszweck dienen. Sie sollen vielmehr die Entstehung eines Gebäudes oder eine Platzgestaltung zu Archiv- und/oder Marketingzwecken dokumentieren. Für die

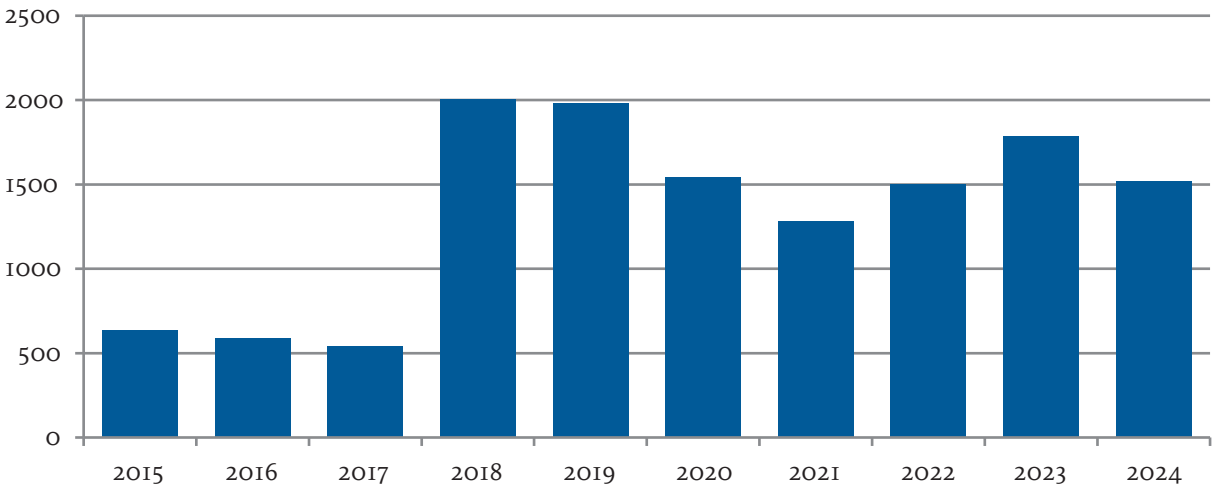


Abbildung 2: Anzahl der Anfragen pro Jahr

Zweckerreichung sind somit keine personenbezogenen Daten notwendig, weshalb diese Videoaufzeichnungen lediglich zulässig sind, wenn die Kameras so eingerichtet sind, dass Personen auf den Aufnahmen nicht identifizierbar sind und letztere daher gar nicht unter die Datenschutzgesetzgebung fallen.

Auch mit einem weiteren Einsatz von Kameras, der nicht unter den klassischen Videoüberwachungszweck fällt, hatte sich die DSS im Berichtsjahr zu befassen. Es handelte sich dabei um Kameras, welche die KfZ-Nummernschilder von Fahrzeugen bei der Ein- und Ausfahrt in eine Tiefgarage erfassen. Die Schranke öffnet sich bei der Einfahrt, wenn nach der Erfassung des Nummernschilds und einem Abgleich mit einer Datenbank (Mitarbeitende) das Kennzeichen dort hinterlegt ist oder sonst ein Ticket gezogen wird, und sie öffnet sich entsprechend bei der Ausfahrt, wenn der Abgleich des erfassten Nummernschilds mit der Datenbank positiv ausfällt oder sonst das Ticket vorgängig bezahlt wurde. Im konkreten Fall stützt sich die gegenständliche Datenverarbeitung auf eine gesetzliche Grundlage. Aus datenschutzrechtlicher Sicht ist dabei zudem zentral, dass es sich ausschliesslich um einen Abgleich handelt und keine weitere Verarbeitung (insbesondere keine Speicherung) durchgeführt wird. Festzuhalten gilt es auch, dass in der Tiefgarage eine datenschutzrechtlich konforme Videoüberwachung in Betrieb ist. Die Datenverarbeitung durch die Kennzeichen-Erfassung stellt daher keinen weiteren tiefergreifenden Eingriff in die Rechte der Betroffenen dar.

Auch mit Videoüberwachungskameras in privaten Wohnräumen beschäftigte sich die DSS. Bei der Nutzung von Kameras im privaten Bereich, insbesondere in privaten Wohnräumen, stellt sich zunächst die Frage nach der Anwendbarkeit der Datenschutzgesetzgebung aufgrund der Haushaltsausnahme. Dabei ist der Zweck der Datenverarbeitung zentral. Werden Aufnahmen zum ausschliesslichen privaten oder persönlichen Gebrauch generiert, ist die DSGVO wie auch das DSG nicht anwendbar. Dies ist zum Beispiel der Fall bei privaten Festen unter der Voraussetzung, dass die Aufnahmen nicht veröffentlicht oder an einen grösseren Kreis von Personen verbreitet werden. Kameras, die hingegen zum Zwecke der Sicherheit installiert werden, implizieren zur Zweckerfüllung eine Datenweitergabe an Polizei oder Versicherungen. Damit ist die Datenschutzgesetzgebung mit all ihren Anforderungen auf sie anwendbar.

Auch bezüglich der Speicherung von Videoaufnahmen war die DSS beratend tätig. So dürfen Videoaufnahmen im Ausland (Drittstaat) gespeichert werden, wenn eine Speicherung grundsätzlich zulässig ist und die Voraussetzungen für einen Auslandsdatentransfer in Drittstaaten erfüllt sind.

Wildtierkameras beschäftigten die DSS in zweifacher Hinsicht. Zunächst stellte sich die Frage, wie ausführlich die Angabe des Verantwortlichen in Zusammenhang mit der Informationspflicht gemäss Art. 13 DSGVO zu erfolgen hat. Bei Jägern handelt es sich um natürliche Personen, die durch diese Informationspflicht ihre persönlichen Kontaktdaten veröffentlichen müssten. Im Rahmen einer Abwägung stellte die DSS daher fest, dass in diesen Fällen ausnahmsweise auf eine vollständige Angabe von Namen und Adresse verzichtet werden kann und stattdessen Vor- oder Nachname mit den Initialen abgekürzt werden dürfen wie auch eine generische E-Mailadresse aufgeführt werden kann. In einem weiteren Fall wurde eine Wildtierkamera als Fotofalle zur Erlangung von Erkenntnissen über Verhalten, Population etc. bestimmter Tiere aufgestellt. Zur Erfüllung dieses Zwecks sind keine personenbezogenen Daten notwendig. Daher sind die Kameras in erster Linie so auszurichten bzw. so auszugestalten, dass diesem Umstand Rechnung getragen wird. Nun wurde durch eine solche Fotofalle ein potentiell strafrechtlich relevantes Verhalten festgestellt. Es stellte sich die Frage, ob diese Daten an die zuständigen Stellen weitergegeben werden dürfen. Ausschlaggebend hierfür waren im konkreten Fall Art. 22 und 24 DSG, welche eine Verarbeitung und Veröffentlichung zu anderen Zwecken regelt. Art. 22 und Art. 24 DSG setzen dabei voraus, dass die personenbezogenen Daten, welche zur Strafverfolgung genutzt werden sollen, ursprünglich zur Erfüllung eines datenschutzrechtlich relevanten Zwecks erhoben wurden. Im konkreten Fall ist der Zweck der Fotofalle das Erfassen von Wildtieren. Die zufälligen Aufnahmen einer Person entsprechen diesem Zweck jedoch nicht bzw. erfüllen gar keinen Zweck. Es fehlt den Aufnahmen in diesem Sinne daher an einem ursprünglichen datenschutzrechtlich relevanten Zweck, weshalb Art. 22 und Art. 24 DSG für den konkreten Fall nicht angewendet werden konnten.

Auch Videoüberwachungen durch Gemeinden beschäftigten die DSS im Berichtsjahr. In diesem Zusammenhang orientiert sich die DSS an einem Urteil des VGH, wonach eine Überwachung von Bereichen, die zum kulturellen und sozialen Austausch und zur Freizeitgestaltung ausgelegt sind, grundsätzlich unzulässig ist. Die DSS setzt daher in solchen Fällen hohe Massstäbe an das berechtigte Interesse wie auch die damit verbundene Verhältnismässigkeitsprüfung.

Auch bei der Frage einer Videoüberwachung in einem Hotel spielte die Erfassung des Freizeitverhaltens eine Rolle. So vertritt die DSS die Ansicht,

dass die Überwachung von Aufenthaltsräumen wie der Lobby unzulässig ist, auch wenn die Rezeption zu bestimmten Zeiten nicht besetzt ist. Die DSS begründet ihre Position damit, dass auch in diesen Situationen die Interessen der Betroffenen, in ihrem Freizeitverhalten nicht überwacht zu werden, überwiegen. Zudem können alternativ Eingangs- oder Durchgangsbereiche überwacht werden, was weniger eingriffsintensiv ist, da man sich dort üblicherweise nicht länger aufhält.

Gleich mehrere Anfragen und Meldungen von Videoüberwachungen in Geschäften gingen bei der DSS im Berichtsjahr ein. Datenschutzrechtlich ist hierbei insbesondere die Wahrung der Privatsphäre der Mitarbeitenden zentral. Bei Videokameras in Geschäften gilt es bezüglich jeder einzelnen Kamera ein objektiv vorliegendes berechtigtes Interesse zu prüfen, welches die Interessen der von den Aufnahmen betroffenen Personen überwiegen muss. Einer umfassenden Videoüberwachung von Geschäften steht die DSS grundsätzlich kritisch gegenüber. Zusätzlich ist noch anzufügen, dass Geschäfte aufgrund ihres Zwecks öffentlich zugängliche Bereiche sind, weshalb eine Videoüberwachung dort nach Art. 5 Abs. 7 DSG bei der DSS meldepflichtig ist.

Nachdem die DSS schon bei der planerischen Ausgestaltung der Videoüberwachung der Landespolizei in Schaan beratend miteinbezogen wurde, entschloss sich die DSS im Berichtsjahr, diese mittlerweile realisierte Videoüberwachung einer eingehenderen Datenschutzüberprüfung zu unterziehen. Ausschlaggebend dafür waren insbesondere der Umfang sowie die Sensitivität der Videoüberwachung. Hinzu kommt, dass im Berichtsjahr bei der DSS eine Beschwerde eines Anwohners des von den Aufnahmen betroffenen Bereichs einging. Es stellte sich insbesondere die Frage, welche Bereiche von den Kameras genau erfasst sind und welche nicht, wie die konkrete technische und organisatorische Ausgestaltung der Videoüberwachung aussieht und wie Informationspflichten umgesetzt werden. Die gegenständliche Überprüfung konnte im Berichtsjahr nicht abgeschlossen werden.

Des Weiteren ging die DSS im Berichtsjahr mehreren Beschwerden gegen konkrete Videoüberwachungsanlagen nach und führte Beratungen bei Unternehmen, Ämtern, Vereinen und Privaten durch. Auffallend war erneut, dass Videoüberwachungen im Nachbarschaftsbereich oft zu langen und sehr emotionalen Streitigkeiten führten. Es erfordert viel Fingerspitzengefühl, die Parteien davon zu überzeugen, dass der Betrieb einer Videoüberwachung klaren rechtlichen Vorgaben zu folgen hat und die Privatsphäre dritter Personen zu respektieren ist.

Insgesamt gingen im Berichtsjahr bei der DSS 22 Meldungen zu neuen, fix installierten Videoüberwachungen ein sowie 10 Meldungen zu Drohnenflügen mit Kameras.

2.3 Verbindliche interne Datenschutzvorschriften

Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules; BCR) sind ein unter dem Kapitel V der DSGVO vorgesehenes Instrument der Datenübermittlung in Drittstaaten, mit welchen eine sichere Datenverarbeitung in Drittstaaten gewährleistet werden soll. Sie bieten sich insbesondere für weltweit tätige Unternehmen mit zahlreichen Tochtergesellschaften in verschiedenen Ländern an und dienen dazu, den Datenschutz in solchen Organisationen auch auf Datenverarbeitungen auszuweiten, im Rahmen derer personenbezogene Daten vom EU/EWR-Raum aus in Drittländer gelangen.

Das Instrument der BCR wurde bereits vor Geltung der DSGVO geschaffen und ist seitdem laufend fortentwickelt worden. Aufgrund seines Erfolges wurde es mit der DSGVO «verrechtlicht» und nochmals konkretisiert. BCR bieten Unternehmen den Vorteil, dass es sich um keine starre Vorgabe von Verpflichtungen handelt, sondern um ein flexibles und adaptierbares Konstrukt, welches ständig weiterentwickelt werden kann und sich somit problemlos auch an neue Gegebenheiten anpassen lässt. Sie müssen jeweils von den nationalen Datenschutzbehörden unter vorgängiger Konsultation des EDSA genehmigt werden.

Die DSGVO sieht vor, dass es für jedes Unternehmen bezüglich Fragen zu den BCR eine federführende Aufsichtsbehörde gibt, welche für die BCR und deren Genehmigungsverfahren die zentrale Ansprechpartnerin ist. Weiters wurden vom EDSA Leitlinien ausgearbeitet, die eine Anleitung für Antragsteller bieten und Inhalte von BCR vorgeben. Um sicherzustellen, dass die Vorgaben für BCR von allen europäischen Datenschutzbehörden möglichst einheitlich angewendet werden, wurde mittlerweile auch eine elektronische Diskussionsplattform eingerichtet und es werden regelmässige Treffen einberufen, an denen offene und strittige Punkte von den Behörden abschliessend behandelt werden.

Ein schon länger bestehendes und viel diskutiertes Thema ist die grosse Arbeitslast der Aufsichtsbehörden bei BCR-Genehmigungsverfahren, bedingt durch die zeitintensive Prüfung von eingereichten BCRs und die nach wie vor hohe Zahl von noch anstehenden BCR-Genehmigungsverfahren. Das Verfahren soll deshalb effizienter gestaltet werden, ohne qualitative Einbussen zu erleiden. So wurde beispielsweise die Möglichkeit geschaffen, dass nach vorgängiger

Absprache die Überprüfung durch die federführende Behörde und die zwei «Co-Reviewer» zeitlich parallel durchgeführt werden. Diese Schritte wurden bisher nacheinander durchgeführt. Durch die Parallelität verspricht man sich nicht nur Zeitersparnisse, sondern auch einen intensiveren und zeitlich koordinierten Austausch bezüglich offener Fragen zwischen den überprüfenden Behörden. Zudem wurde im Berichtsjahr die EDSA-interne Ausarbeitung eines Prozesses zur Begleitung der Genehmigungsverfahren weitergeführt.

Aus nationaler Perspektive ist zu berichten, dass das im Jahr 2022 begonnene BCR-Genehmigungsverfahren eines liechtensteinischen Unternehmens im Berichtsjahr abgeschlossen werden konnte. So hat der EDSA zu den vorbereiteten BCR Stellung genommen und die DSS konnte die entsprechende Genehmigung erteilen. Gegen Ende des Berichtsjahres meldete ein weiteres liechtensteinisches Unternehmen Interesse an einem BCR-Verfahren bei der DSS an. Die offizielle Einleitung des Verfahrens wird 2025 erfolgen.

2.4 Auswahl konkreter rechtlicher Fragen

Die DSS hat im Berichtsjahr wieder zahlreiche Anfragen zur Klärung und Beurteilung von rechtlichen Themen im Datenschutz erhalten. Nachfolgend werden daraus einige kurz dargestellt.

Praxisänderung bei Trauerspenden bzw. Jubiläumsspenden

Aufgrund der rechtlichen Fortentwicklung in Europa passte die DSS im Berichtsjahr ihre Praxis bezüglich der Frage an, wie eine Spenden empfangende Organisation (z.B. gemeinnützige Stiftung, soziale Institution, Verein u.ä.) im Fall von Trauerspenden Angaben zu den spendenden Personen datenschutzkonform einer Trauerfamilie bekannt geben kann.

Wie bisher ist die Weitergabe des Namens (und der Adresse) einer spendenden Person an die Trauerfamilie mit ihrer ausdrücklichen Einwilligung zulässig. Die Einholung einer solchen ausdrücklichen Einwilligung aller spendenden Personen kann sich jedoch recht schwierig gestalten, obwohl vermutlich die wenigsten spendenden Personen wirklich anonym bleiben wollen (sonst hätten sie ja auch ohne Bezug zur Trauerfamilie spenden können). Deshalb erachtet es die DSS neu ebenfalls als zulässig, dass eine Spenden empfangende Organisation einer spendenden Person ein Dankesschreiben schickt und ihr mitteilt, dass sie ihren Namen (und ihre Adresse) an die Trauerfamilie weitergeben wird, sofern sie sich nicht binnen drei Wochen bei der Organisation meldet und Widerspruch dagegen einlegt. Es muss der spendenden Person also von der Organisation nach Information über die anstehende Datenweitergabe eine angemessene Frist gewährt werden, innerhalb derer sie sich bei ihr melden und die Weitergabe ablehnen könnte («opt-out»). Mit diesem Vorgehen ist aus Datenschutz-Sicht ebenfalls ein Ausgleich zwischen den Interessen von Trauerfamilie, Spenden empfangender Organisation und spendender Person auf geeignete Weise möglich.

Von dieser Datenweitergabe an die Trauerfamilie ausgenommen ist allerdings der konkrete Spendenbetrag pro spendende Person. Dafür bräuchte es immer noch die ausdrückliche Einwilligung derselben. Ansonsten darf die Trauerfamilie von der Spenden empfangenden Organisation nur über den Totalbetrag der eingegangenen Spenden informiert werden. Dieselbe Praxis gilt auch für den Fall von Jubiläumsspenden etwa anlässlich eines runden Geburtstags.

Zulässigkeit von Telefonaufzeichnungen

Für Finanzintermediäre, darunter Banken, Wertpapierfirmen und andere unter die Richtlinie 2014/65/EU über Märkte für Finanzinstrumente (MiFID II) fallende Institutionen, gelten strikte Vorgaben zur Aufzeichnung von Telefongesprächen. Gemäss Art. 16 Abs. 7 MiFID II müssen Telefongespräche, die im Zusammenhang mit der Annahme, Übermittlung und Ausführung von Kundenaufträgen sowie Eigengeschäften stehen, verpflichtend aufgezeichnet werden. In Liechtenstein wurden diese Vorgaben durch das Wertpapierdienstleistungsgesetz (WPDG) und die Bankenverordnung (BankV) umgesetzt. Die gesetzliche Aufzeichnungspflicht beschränkt sich dabei allerdings ganz klar auf Gespräche zu Finanztransaktionen; allgemeine Service- und Beratungsgespräche sind davon nicht umfasst.

Gleichzeitig setzt auch die DSGVO klare Grenzen: Pauschale Aufzeichnungen von Telefongesprächen sind unzulässig, da sie gegen die Grundsätze der Rechtmässigkeit, Zweckbindung und Datenminimierung gemäss Art. 5 Abs. 1 Bst. a, b und c DSGVO verstossen. Für nicht-transaktionsbezogene Gespräche, die sich weder auf die erwähnte gesetzliche Aufzeichnungspflicht noch (in äusserst seltenen Fällen) auf eine Notwendigkeit zur Vertragserfüllung als Rechtsgrundlage stützen können, ist daher in der Regel eine aktive und freiwillige Einwilligung der betroffenen Person erforderlich. Das blosse Fortsetzen eines Gesprächs nach einem Hinweis auf die Aufzeichnung reicht hierfür nicht aus. Finanzintermediäre müssen daher standardmässig insbesondere mit technischen und organisatorischen Massnahmen (z.B. einer entsprechenden Telefonanlage) sicherstellen, dass Aufzeichnungen ausschliesslich in gesetzlich vorgese-

henen Fällen, bei vertraglichem Erfordernis oder bei expliziter Einwilligung des Anrufers erfolgen und die Datenschutzvorgaben der DSGVO konsequent eingehalten werden.

Zugriff auf E-Mail-Accounts von ehemaligen Mitarbeitenden

Wenn Mitarbeitende aus dem Unternehmen ausscheiden, stellt sich sehr häufig die Frage, wie mit ihren E-Mail-Accounts umzugehen ist und ob der Arbeitgeber darauf zugreifen darf. Die DSS hat in mehreren Fällen die Zulässigkeit des Zugriffs bejaht, wenn die folgenden Voraussetzungen erfüllt sind: Der/dem Mitarbeitenden wurde Gelegenheit gegeben, private E-Mails auszusortieren und private Kontakte entsprechend zu informieren. In kritischen Fällen können bei diesem «Aufräumen» des E-Mail-Accounts auch der Datenschutzbeauftragte oder ein Vorgesetzter etc. anwesend sein, wenn Gefahr besteht, dass etwa geschäftliche E-Mails unrechtmässig gelöscht werden könnten. Zudem sollte eine entsprechende Abwesenheitsnotiz im E-Mail-Account eingerichtet werden. Daraufhin kann der Zugriff des Arbeitsgebers durch Art. 6 Abs. 1 Bst. f DSGVO gerechtfertigt sein, wenn der Arbeitgeber konkrete unternehmerische Interessen am Zugriff geltend machen kann. Diese konkreten Interessen bestimmen auch die Dauer der Speicherung des E-Mail-Accounts. Sobald die Aufbewahrung durch keine konkreten unternehmerischen Interessen, etwa der Abwicklung eines Auftrags, mehr gerechtfertigt werden können, ist dieser zu löschen.

Datenoffenlegung durch Gemeinden

Mehrere Gemeinden hatten im Berichtsjahr Anfragen von privaten Kinderbetreuungsstätten bzw. Kitas erhalten, die sämtliche Adressen von Kindern bzw. deren Eltern in der Gemeinde wünschten, um auf ihr neues Kita-Angebot hinzuweisen bzw. dafür zu werben.

Datenschutzrechtlich einschlägig ist hierfür die Verordnung vom 11. Dezember 2018 über die Offenlegung bestimmter personenbezogener Daten durch die Gemeinden, LGBl. 2018/454, das heisst konkret Art. 4 zu Gruppenanfragen, welcher unter anderem verlangt, dass «der Gesuchsteller ein berechtigtes Interesse glaubhaft macht. Dies ist insbesondere dann der Fall, wenn die personenbezogenen Daten für politische, kulturelle, soziale, wissenschaftliche oder sonstige ideelle Zwecke erforderlich sind». In Bezug auf diese Bedingung ist fraglich, ob ein berechtigtes Interesse der Kitas vorliegt. Zwar verfolgt eine Kita einen Zweck, der grundsätzlich im sozialen Bereich liegt, aber im konkreten Fall ging es jeweils um ein privatwirtschaftliches Unternehmen und insbesondere die werbliche Ansprache der Betroffenen mit dem Ziel, die Dienstleistung der Kita zu verkaufen. Würde man dies als sozialen Zweck verstehen, könnten in der Folge zahlreiche privatwirtschaftliche Unternehmen, welche im weitesten Sinn eine soziale Dienstleistung oder ein soziales Produkt verkaufen, Adressen für Werbezwecke von einer Gemeinde verlangen, was nicht im Sinne des Gesetzgebers sein kann.

Zudem ist zu prüfen, ob «die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Offenlegung hat; und die betroffene Person nicht von ihrem Widerspruchsrecht Gebrauch gemacht hat.» Die Vermeidung von unerwünschter Werbung stellt jedoch ein schutzwürdiges Interesse betroffener Personen dar und ist somit von dieser Bestimmung erfasst. Folglich kann eine Gemeinde einer privaten Kita keine Auskunft über personenbezogene Daten von Kindern bzw. deren Eltern für werbliche Zwecke geben. Die DSS empfiehlt daher, Werbung mittels Plakaten beispielsweise an Spielplätzen, bei der Gemeinde oder in Spielgruppen zu machen, auf Zeitungsinserate zurückzugreifen oder auch Flyer zu verteilen.

Veröffentlichung von Fotos bewohnter Wohnungen durch Makler – Frage der Rechtsgrundlage

Fotos von (bewohnten) Wohnräumen gelten nach der DSGVO als personenbezogene Daten, da sie Rückschlüsse auf die Lebensgewohnheiten der Bewohner zulassen. Für die Erstellung und Veröffentlichung solcher Fotos ist deshalb eine Rechtsgrundlage gemäss Art. 6 DSGVO erforderlich. Bei der Bestimmung dieser Rechtsgrundlage ist grundsätzlich zu unterscheiden, ob es sich bei den Bewohnern um Mieter oder Eigentümer der fraglichen Wohnung handelt. Im Falle von Mietern ist vom Makler vor dem Erstellen und Veröffentlichen von Fotos deren Einwilligung gemäss Art. 7 DSGVO einzuholen. Die DSS empfiehlt, diese Einwilligung aus Beweisgründen schriftlich einzuholen. Zudem hat der Makler die Mieter gemäss Art. 13 DSGVO zu informieren und sie insbesondere auf die konkrete Verwendung der Fotos (gedrucktes oder online verfügbares Exposé) und ihr Widerrufsrecht hinzuweisen. Wichtig ist zudem, dass bei der Erstellung der Fotos darauf geachtet wird, dass aus den Fotos keine Rückschlüsse auf besondere Kategorien personenbezogener Daten gezogen werden können, sprich beispielsweise keine religiösen Gegenstände abgebildet sind. Dies wäre nur mit einer zusätzlichen und speziell dafür erteilten ausdrücklichen Einwilligung gemäss Art. 9 Abs. 2 Bst. a DSGVO zulässig.

Handelt es sich bei den Bewohnern um die Eigentümer der Wohnung, kann – je nach Inhalt – der Makler-

vertrag gemäss Art. 6 Abs. 1 Bst. b DSGVO als Rechtsgrundlage für die Erstellung und Veröffentlichung von Fotos herangezogen werden. Aber auch hier sind die weiteren Grundsätze der DSGVO zu beachten und bei den Aufnahmen Rückschlüsse auf besondere Kategorien von personenbezogenen Daten zu vermeiden, ausser es wird dafür eine ausdrückliche Einwilligung gemäss Art. 9 Abs. 2 Bst. a DSGVO eingeholt.

Dieselben Überlegungen fanden auch Anwendung im Falle eines Bausachverständigen, der seine Gutachten mit Fotos der überprüften Wohnungen untermauerte.

2.5 Auswahl konkreter technischer Fragen

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

Welche Herausforderungen und Pflichten ergeben sich für Webseitenbetreiber bei der Einholung von Einwilligungen für einwilligungspflichtige Verarbeitungsvorgänge, insbesondere im Zusammenhang mit Cookies und Tracking-Technologien?

Webseitenbetreiber als Verantwortliche müssen sicherstellen, dass sie bei einwilligungspflichtigen Verarbeitungsvorgängen (z.B. beim Einsatz technisch nicht erforderlicher Cookies oder bei der Weitergabe von Daten an Dritte) vor der eigentlichen Verarbeitung die Einwilligung der Webseitenbesucher einholen. Zur Einholung der Einwilligung hat sich in der Praxis der Einsatz von sogenannten Einwilligungsmanagement-Tools, häufig auch als Cookie-Banner bezeichnet, etabliert. Diese können in der Regel als Cloud-Lösung oder als lokal ausführbare Software in Webseiten eingebunden werden.

Mittlerweile gibt es zahlreiche Anbieter von Einwilligungsmanagement-Tools auf dem Markt und diese werben häufig mit der DSGVO-Konformität ihrer Angebote. Nach den Erfahrungen der DSS ist der Einsatz solcher Tools jedoch häufig mit datenschutzrechtlichen Mängeln behaftet. Einer der am häufigsten beobachteten Fehler ist, dass viele Tools technisch nicht sicherstellen, dass während der Einblendung von Cookie-Bannern keine weitergehenden (Tracking-)Skripte ausgeführt und/oder technisch nicht erforderliche Cookies im Browser gespeichert werden. So werden häufig bereits beim blossen Aufruf einer Webseite – und noch bevor man im Cookie-Banner irgendeine Einwilligung erteilen kann – personenbezogene Daten des Webseitenbesuchers (u.a. die IP-Adresse) an Dritte übermittelt und/oder technisch nicht erforderliche Cookies im Browser gespeichert. Zudem sind Cookie-Banner häufig unnötig komplex gestaltet (z.B. keine einfache Ablehnungsmöglichkeit oder voreingestellte Einwilligungsoptionen) oder enthalten keine klaren Informationen über Art und Zweck der verwendeten Cookies und Tracking-Technologien. Nicht zuletzt aufgrund dieser erheblichen technischen Herausforderungen bei der korrekten Einholung der Einwilligung ist Webseitenbetreibern zu empfehlen, sorgfältig zu prüfen, ob ein Cookie-Banner für die eigene Webseite überhaupt erforderlich ist (siehe dazu die Ausführungen auf der Internetseite der DSS).

Um den eigenen Aufwand gering zu halten, empfiehlt es sich zudem, auf einwilligungspflichtige Cookies und Verarbeitungen bzw. solche nutzenden Applikationen so weit wie möglich zu verzichten. Dies kann einerseits durch den Einsatz von datenschutzfreundlicheren Lösungen bei der Einbindung von externen (Medien-)Inhalten (z.B. durch lokale Einbindung von Schriften oder Videos) und bei der sogenannten Reichweitenanalyse erreicht werden. Andererseits kann beispielsweise auch mit der gezielten Verlinkung auf Webseiten anderer Anbieter (z.B. Kartendienste), wodurch ein Besucher beim Anklicken von der eigenen Webseite weggeleitet wird, die eigene Verantwortlichkeit für allfällige einwilligungspflichtige Cookies und Datenverarbeitungen vermieden werden. Allerdings gilt dies nur, wenn der Link nicht zu einem Nutzerprofil oder ähnlichem des Verantwortlichen führt (z.B. auf Social Media), wo dann unter Umständen wieder eine gemeinsame Verantwortlichkeit für die Datenverarbeitung besteht.

Was sind häufige Ursachen für Datenschutzverletzungen bei Webanwendungen und durch welche technischen und organisatorischen Massnahmen können diese verhindert werden?

Immer wieder erhält die DSS Meldungen von Verletzungen der Vertraulichkeit (sensibler) personenbezogener Daten, da diese nur unzureichend durch technische und organisatorische Massnahmen, wie etwa Verschlüsselung bei der Speicherung, verschlüsselte Datenübertragung oder die Vergabe möglichst restriktiver Zugriffsrechte, geschützt waren. Besondere Vorsicht ist beim Datenaustausch über Browser geboten. Gerade bei Webanwendungen kommt es nach den Erfahrungen der DSS häufiger vor, dass schützenswerte Daten, zum Beispiel durch falsch konfigurierte Zugriffsrechte, von unberechtigten Personen unbefugt eingesehen und womöglich kopiert werden könnten. Sind keine weiteren Zugriffsbeschränkungen (z.B. Passworteingabe) vorgesehen, könnten etwa Nutzerdaten aus Kontaktformularen oder Bewerberdaten aus Online-Bewerbungstools durch einfachen Abruf der entsprechenden Webadressen abgerufen werden.

Es lohnt sich daher, die IT- und Datensicherheit von Webapplikationen und Webservern von Zeit zu Zeit zu überprüfen bzw. überprüfen zu lassen, da diese in der Regel Veränderungen unterliegen (z.B. System-Update oder Weiterentwicklungen) und technische Massnahmen wie etwa Zugriffsrechte wieder neu angepasst werden müssen.

Welche datenschutzrechtlichen Vorgaben und Sicherheitsvorkehrungen musste Google bei der Einführung von Google Street View in Liechtenstein beachten und welche Rechte haben die Betroffenen?

Nachdem bereits alle anderen EU/EWR-Mitgliedstaaten von Google in «Google Street View» aufgenommen wurden, folgte im Berichtsjahr auch Liechtenstein. Damit können nun auch für Liechtenstein fotografische Ansichten von Strassen, Wegen und umliegenden Gebäuden in Google Maps dargestellt werden. Die Aufnahmen dafür erfolgten zwischen August und September 2024 mit speziell gekennzeichneten Fahrzeugen von Google.

Bezüglich der Erstellung und Veröffentlichung dieser Bilder hat Google eng mit den Datenschutzbehörden in Europa zusammengearbeitet, um die damit verbundene Datenverarbeitung rechtskonform zu gestalten. So wurde auch die DSS von Google vorgängig konsultiert und konnte die datenschutzrechtlichen Anforderungen an das Projekt in Liechtenstein klarstellen. Zu den wichtigsten Sicherheitsmassnahmen gehörte dabei die Beschränkung der Aufnahmen auf nur von der Strasse aus einsehbare Bereiche von Grundstücken sowie die automatisierte Verpixelung (Unkenntlich-Machung) der Gesichter und Kennzeichen von zufällig anwesenden Passanten und Fahrzeugen vor der Veröffentlichung der Bilder in «Google Street View». Dies entspricht einer Löschung der personenbezogenen Daten. Die Verpixelung geschieht nach einer gewissen Übergangszeit ausserdem auf den Rohdaten der Bilder, womit auch eine Verpixelung in künftigen Darstellungen gewährleistet ist. Die Aufnahmedaten wurden zudem bereits im Fahrzeug auf verschlüsselten Festplatten gespeichert, sodass diese auch auf dem Transportweg in die Rechenzentren von Google vor unbefugtem Zugriff geschützt waren. Die DSS verlangte darüber hinaus von Google vor Beginn der Aufnahmen eine breite Information der liechtensteinischen Bevölkerung in den lokalen Medien über das Projekt, den geplanten Ablauf sowie die Rechte der Betroffenen, was über einen entsprechenden Bericht im «Vaterland» am 16. Juli 2024 erfolgte. Daneben informierte die DSS auch selbst auf ihrer Internetseite sowie in einem Newsletter.

Da als Rechtsgrundlage für das Erstellen und Veröffentlichen der Bilder (auf denen natürliche Personen nicht im Fokus stehen) das berechtigte (wirtschaftliche) Interesse von Google gemäss Art. 6 Abs. 1 Bst. f DSGVO dient, haben betroffene Personen gemäss Art. 21 DSGVO auch das Recht, dieser Datenverarbeitung jederzeit zu widersprechen und die Löschung bzw. Verpixelung von allenfalls noch nicht automatisiert verpixelten Gesichtern und Autokennzeichen sowie zusätzlich von ganzen Körpern, Fahrzeugen oder Hausfassaden zu verlangen. Dies kann über die «Problem melden»-Funktion im Menü innerhalb von «Google Street View» beantragt werden und wird von Google im Regelfall ohne weiteren Nachweis umgesetzt.

2.6 Wichtigste EuGH-Entscheidungen 2024

Nachdem die Entscheidungen des EuGH für die Beurteilungen 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 datenschutzrechtlich bedeutendsten Entscheidungen des EuGH im Berichtsjahr hingewiesen.

EuGH, 14. März 2024, C-46/23: Budapest Főváros v. Nemzeti (Befugnisse der Aufsichtsbehörde)

Gemäss EuGH ist Art. 58 Abs. 2 Bst. d und g DSGVO dahingehend auszulegen, dass die Datenschutz-Aufsichtsbehörde eines Mitgliedstaats den Verantwortlichen oder Auftragsverarbeiter in Ausübung ihrer in diesen Bestimmungen vorgesehenen Abhilfebefugnisse selbst dann zur Löschung unrechtmässig verarbeiteter personenbezogener Daten anweisen darf, wenn die betroffene Person – etwa in Unkenntnis der tatsächlich verarbeiteten Daten – keinen entsprechenden Antrag auf Löschung nach Art. 17 Abs. 1 DSGVO gestellt hat. Eine solche Löschanordnung kann sich dabei sowohl auf bei der betroffenen Person erhobene als auch auf aus einer anderen Quelle stammende Daten beziehen.

Der EuGH hält fest, dass es für Datenschutz-Aufsichtsbehörden zur Erfüllung ihrer Aufgabe, die Anwendung der DSGVO zu überwachen und durchzusetzen, erforderlich ist, dass sie über geeignete und wirksame Befugnisse verfügen, um gegen Verstösse effektiv vorgehen zu können. Diese umfassen deshalb auch Untersuchungen und Sanktionen von Amtes wegen, ohne dass ein Betroffener dies zuvor mit einer Beschwerde beantragt hätte.

Die Frage des Auskunftsrechts und insbesondere des Rechts auf Kopie ist eine der am häufigsten gestellten Fragen an die DSS und ist folglich auch regelmässig Gegenstand von Beschwerden. Die DSS weist dabei insbesondere auf zwei Aspekte hin, die vom EuGH in diesem Urteil bestätigt wurden: Einerseits muss eine betroffene Person keinen Grund für ihr Auskunftsgesuch nach Art. 15 DSGVO angeben. Andererseits steht es der verantwortlichen Stelle mit Blick auf die Kopie aber frei zu entscheiden, was von einer Kopie konkret umfasst sein muss. Dabei darf sich die verantwortliche Stelle von der Frage leiten lassen, ob die Kopie dazu dienen kann, dass die betroffene Person auf Grundlage der erhaltenen Kopie weitere Betroffenenrechte wie Berichtigung oder Löschung geltend machen kann. Nur wenn diese Frage mit Ja zu beantworten ist, besteht die Verpflichtung, eine Kopie der entsprechenden Daten auszuhändigen. Im Berichtsjahr beurteilte die DSS mehrere Anfragen, ob ein ehemaliger Mitarbeitender Anspruch auf eine Herausgabe sämtlicher von ihm im Beschäftigungskontext verfassten und empfangenen E-Mails hat, entlang dieses Grundsatzes. Die DSS verneinte diesen Anspruch, da in den untersuchten Fällen auszuschliessen war, dass die betroffene Person im Hinblick auf diese geschäftlichen E-Mails ein Betroffenenrecht hätte geltend machen können.

EuGH, 11. Juli 2024, C 757/22: Meta v. Verbraucherzentrale (Datenschutzhinweise sowie Verbandsklagebefugnis)

In erster Linie hatte sich der EuGH in dieser Rechtssache mit der Verbandsklagebefugnis zu befassen, die von ihm bei DSGVO-Verstössen bereits in der Vergangenheit mehrfach bejaht worden war. Offen war nach Ansicht des vorlegenden Gerichts allerdings noch die Frage, ob ein Verstoss gegen die Informationspflichten nach Art. 13 DSGVO in den Anwendungsbereich des Art. 80 Abs. 2 DSGVO fällt. Art. 80 Abs. 2 DSGVO verlangt nämlich, dass eine Verbandsklage nur dann zulässig ist, wenn eine Rechtsverletzung beim Betroffenen «infolge einer **Verarbeitung**» eingetreten sei.

Das Gericht bestätigt die in den Schlussanträgen des Generalanwalts vertretene Rechtsauffassung, wonach die Informationspflicht gemäss DSGVO nicht als eigenständige Datenverarbeitung zu qualifizieren ist. Nach Ansicht des Gerichts ist jedoch die Bereitstellung der Informationen gemäss den Art. 12 ff. DSGVO eine wesentliche Voraussetzung für die Rechtmässigkeit der Datenverarbeitung im Sinne von Art. 6 DSGVO.

Wird – wie im vorliegenden Fall – die Verarbeitung personenbezogener Daten auf die Einwilligung der betroffenen Person gestützt, so ist eine transparente Unterrichtung dieser bereits integraler Bestandteil einer rechtmässigen Verarbeitung. Das Gericht hält weiter fest, dass eine Datenverarbeitung, die unter Missachtung der Informationspflichten oder -rechte erfolgt, dazu führt, dass die betroffene Person in ihren Rechten «durch die Verarbeitung» verletzt wird und eine Verbandsklage somit zulässig ist.

Für Liechtenstein ist die Frage der Verbandsklagebefugnis nicht von allzu grosser Bedeutung, da bislang keine solchen Klagen eingebracht wurden. Hingegen ist die Entscheidung in Bezug auf die Auswirkungen einer unterlassenen oder nicht vollständigen Information nach Art. 13 DSGVO auf die Rechtmässigkeit einer Datenverarbeitung nicht zu unterschätzen. Damit trennt der EuGH die (formelle), zeitlich der jeweiligen Datenverarbeitung vorgelagerte Informationserteilung und die eigentliche Datenverarbeitung nicht mehr ganz, sondern erachtet das Fehlen der ersteren als Grund für die Rechtswidrigkeit der Datenverarbeitung an sich. Zweifelsfrei wird damit der Datenschutz weiter gestärkt. Was dies in der Praxis bedeutet, ist allerdings noch nicht klar und bleibt abzuwarten. Auf jeden Fall sollten Verantwortliche bei der Einhaltung der Informationspflicht noch umsichtiger sein und ihr grösstes Augenmerk schenken.

EuGH, 12. September 2024, C-17/22: HTB v. Müller, und C-18/22: Ökorenta v. WealthCap (Enge Auslegung des berechtigten Interesses; Rechtsprechung als rechtliche Verpflichtung)

Eine Verarbeitung kann nur dann auf ein berechtigtes Interesse gemäss Art. 6 Abs. 1 Bst. f DSGVO gestützt werden, wenn sie zur Verwirklichung des berechtigten Interesses absolut notwendig ist und unter Würdigung aller relevanten Umstände die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person(en) gegenüber diesem berechtigten Interesse nicht überwiegen.

Eine rechtliche Verpflichtung als Rechtsgrundlage für eine bestimmte Datenverarbeitung kommt gemäss EuGH auch in Betracht, wenn sie sich aus der Rechtsprechung eines Mitgliedstaats ergibt, sofern diese Rechtsprechung klar und präzise ist, ihre Anwendung für die

Rechtsunterworfenen vorhersehbar ist und sie ein im öffentlichen Interesse liegendes Ziel verfolgt, zu dem sie in einem angemessenen Verhältnis steht.

Bislang spielte die Rechtsprechung als Rechtsgrundlage für eine Datenverarbeitung in der liechtensteinischen Praxis keine Rolle und wird wohl auch künftig maximal in Ausnahmefällen zum Tragen kommen. Von wesentlich grösserer Tragweite ist allerdings die Auslegung des Begriffs «erforderlich» durch den EuGH. Das Kriterium der Erforderlichkeit spielt eine wesentliche Rolle für die Beurteilung der Rechtmässigkeit einer Datenverarbeitung gemäss Art. 6 Abs. 1 Bst. b-f DSGVO. Der EuGH präzisiert nun dieses Element, indem er ausführt, dass «eine Verarbeitung nur dann als zur Wahrung der berechtigten Interessen eines Dritten erforderlich im Sinne dieser Bestimmung angesehen werden kann, wenn sie zur Verwirklichung eines solchen berechtigten Interesses **absolut notwendig** ist». Der Zusatz der «absoluten Notwendigkeit» erhöht somit die Voraussetzungen für die Inanspruchnahme der berechtigten Interessen und wird auch von der DSS künftig zu berücksichtigen sein.

EuGH, 26. September 2024, C-768/21: TR v. Land Hessen (Entscheidungsspielraum der Aufsichtsbehörde)

Die Datenschutz-Aufsichtsbehörde ist gemäss EuGH nicht verpflichtet, in jedem Fall eines Verstosses gegen die DSGVO eine Abhilfemassnahme gemäss Art. 58 Abs. 2 DSGVO zu ergreifen und insbesondere eine Geldbusse zu verhängen.

So sind Art. 57 Abs. 1 Bst. a und f, Art. 58 Abs. 2 sowie Art. 77 Abs. 1 DSGVO nicht dahingehend auszulegen, dass die Aufsichtsbehörde im Fall der Feststellung einer Verletzung des Schutzes personenbezogener Daten verpflichtet ist, nach Art. 58 Abs. 2 eine Abhilfemassnahme zu ergreifen, insbesondere eine Geldbusse zu verhängen, wenn ein solches Einschreiten nicht geeignet, erforderlich oder verhältnismässig ist, um der festgestellten Unzulänglichkeit abzuhelfen und die umfassende Einhaltung dieser Verordnung zu gewährleisten.

Die betroffene Person einer Datenschutzverletzung hat folglich nicht ohne weiteres Anspruch auf eine bestimmte Handlung der Aufsichtsbehörde.

Diese Entscheidung des EuGH ist von grosser Bedeutung für die Aufsichtstätigkeit der DSS. Wiederholt forderten Beschwerdeführer die DSS im Rahmen ihrer Beschwerde nach Art. 77 DSGVO vehement dazu auf, eine Geldbusse zu verhängen. In Einzelfällen wurde gar mit Amtshaftungsklagen gedroht, sollte die DSS keine Geldbusse verfügen. Bislang beharrte die DSS auf ihrem Recht, unabhängig von Einflussnahme der Parteien die von ihr als adäquat eingeschätzten Abhilfemassnahmen zu ergreifen. Dieses Urteil des EuGH bestätigt somit die Unabhängigkeit und freie Entscheidung der Aufsichtsbehörden und wird von der DSS sehr begrüsst.

EuGH, 4. Oktober 2024, C-507/23: A v. Patērētāju (Entschuldigung als Ersatz eines immateriellen Schadens)

Gemäss EuGH reicht ein Verstoss gegen Bestimmungen der DSGVO für sich genommen nicht aus, um einen «Schaden» im Sinne von Art. 82 Abs. 1 DSGVO darzustellen.

Ist jedoch ein Schaden eingetreten, so kann auch eine Entschuldigung einen angemessenen Ersatz für einen immateriellen Schaden darstellen, insbesondere, wenn es nicht möglich ist, die Lage vor dem Eintritt des Schadens wiederherzustellen. Dies bedingt jedoch, dass diese Form des Schadenersatzes geeignet ist, den der betroffenen Person entstandenen Schaden in vollem Umfang auszugleichen.

Die Haltung und Beweggründe des Verantwortlichen dürfen jedoch bei der Bemessung des Schadenersatzes keine Berücksichtigung finden. Insbesondere darf der betroffenen Person deswegen kein geringerer Schadenersatz gewährt werden als der Schaden, der ihr konkret entstanden ist.

Nachdem in Liechtenstein bislang keine Schadenersatzklagen nach Art. 82 DSGVO entschieden wurden, spielte die Entschuldigung in solchen Fällen keine Rolle. Hingegen kam ihr in zahlreichen Beschwerdefällen vor der DSS grosse Bedeutung zu, erlaubte sie es doch häufig, eine einvernehmliche Lösung zu finden. Die Erfahrung zeigt, dass es für viele betroffene Personen wichtig ist, dass verantwortliche Stellen, denen ein Fehler unterlaufen ist, diesen einsehen und Massnahmen für die Zukunft treffen.

EuGH, 4. Oktober 2024, C-621/22: Koninklijke v. niederländische Datenschutzbehörde (Enge Auslegung des berechtigten Interesses)

Gemäss EuGH setzt Art. 6 Abs. 1 Bst. f DSGVO voraus, dass das berechtigte Interesse nicht mit einem milderen Mittel als der geplanten Datenverarbeitung erreicht werden kann. Die Erforderlichkeit einer bestimmten Datenverarbeitung des Verantwortlichen ist jeweils nur dann zu bejahen, wenn keine zumutbaren Mittel vorliegen, die ebenso geeignet sind und weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen eingreifen.

Auch ein rechtskonformes, wirtschaftliches Interesse kann ein berechtigtes Interesse des Verantwortlichen darstellen.

Wie bereits im Urteil vom 12. September 2024, C-17/22 und C-18/22, befasste sich der EuGH mit dem berechtigten Interesse gemäss Art. 6 Abs. 1 Bst. f DSGVO und erhöhte die Voraussetzungen dafür erneut. Dieses Mal hielt er fest, dass «was zweitens die Voraussetzung der Erforderlichkeit der Verarbeitung personenbezogener Daten zur Verwirklichung des wahrgenommenen berechtigten Interesses angeht, so verlangt diese vom vorlegenden Gericht, zu prüfen, ob das berechtigte Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise **ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen [...] eingreifen**». Somit hat im Rahmen der Anwendung des Art. 6 Abs. 1 Bst. f DSGVO auch eine Prüfung zu erfolgen, ob ein gelinderes Mittel als Alternative verfügbar wäre. Auch diese Präzisierung bzw. Stärkung des Datenschutzes wird die DSS künftig in ihre Abwägungen einfliessen lassen müssen.

EuGH, 4. Oktober 2024, C-21/23: ND v. DR (Gesundheitsdaten bei Online-Arzneimittelbestellungen; DSGVO und Wettbewerbsrecht)

In diesem Urteil stellte der EuGH zunächst fest, dass sämtliche eingegebenen Bestelldaten einer Online-Arzneimittelbestellung zu Gesundheitsdaten gemäss Art. 9 Abs. 1 DSGVO werden, also zum Beispiel auch eine Adresse.

Die DSGVO steht zudem der wettbewerbsrechtlichen Verfolgung von Datenschutzverstössen nicht entgegen. Nach Ansicht des EuGH trägt die Unterlassungsklage eines Mitbewerbers zur Einhaltung der materiellen Bestimmungen der DSGVO bei und stärkt die Rechte der betroffenen Personen ebenso wie ein hohes Schutzniveau, auch wenn die Unterlassungsklage dem Ansinnen nach lediglich einen lauteren Wettbewerb sicherstellen wollte.

Mit diesem Urteil verschärft der EuGH die datenschutzrechtlichen Anforderungen an den Online-Handel. Online-Apotheken müssen den Gesundheitsdatenschutz einhalten, auch bei Präparaten, die nur apotheken- und nicht rezeptpflichtig sind.

Dieses Urteil des EuGH entspricht seiner Tendenz, den Anwendungsbereich der besonderen Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) zu erweitern. Es ist als Appell zu verstehen, insbesondere bei der Wahl der Rechtsgrundlage darauf zu achten, dass die Verarbeitung besonderer Datenkategorien auch eine Rechtsgrundlage gemäss Art. 9 Abs. 2 DSGVO benötigt. Der in der Praxis bedeutendste Unterschied zu den Rechtsgrundlagen gemäss Art. 6 Abs. 1 DSGVO ist, dass Art. 9 Abs. 2 DSGVO den Vertrag nur unter ganz bestimmten Voraussetzungen als Rechtsgrundlage gelten lässt, während Art. 6 Abs. 1 Bst. b DSGVO jeglichen Vertrag zwischen einer betroffenen Person und einem Verantwortlichen als Erlaubnistatbestand erachtet, solange die Datenverarbeitung für dessen Erfüllung erforderlich ist. Verantwortliche sollten somit insbesondere in dieser Hinsicht Vorsicht walten lassen und über allfällige Rechtsgrundlagen nach Art. 9 Abs. 2 DSGVO auch in der Information gemäss Art. 13 DSGVO Auskunft erteilen.

EuGH, 4. Oktober 2024, C-446/21: Schrems v. Meta (Grundsätze der Datenverarbeitung; Verwendung von durch die betroffene Person selbst veröffentlichten personenbezogenen Daten)

Der EuGH stellte fest, dass selbst bei einer grundsätzlichen Einwilligung in die Verarbeitung von personenbezogenen Daten keine grenzenlose Verarbeitung dieser Daten zum Zweck der personalisierten Werbung vorgenommen werden darf. So darf eine Verarbeitung hinsichtlich der Datenmenge und zeitlichen Dauer nicht unbeschränkt sein, sondern findet ihre Grenzen in den Grundsätzen von Art. 5 DSGVO zu Zweckbezogenheit, Datenminimierung und Speicherbegrenzung. Was genau aber eine angemessene Speicherfrist für einen bestimmten Zweck ist (vorliegend die Schaltung personalisierter Werbung), muss jeweils im Einzelfall und gegebenenfalls von den nationalen Gerichten geklärt werden.

Ausserdem bewirkt eine offensichtlich öffentlich gemachte Äusserung nach Art. 9 Abs. 2 Bst. e DSGVO gemäss EuGH zwar die Rechtmässigkeit der Verarbeitung genau dieser Daten. Die Bestimmung ist jedoch eng auszulegen und erlaubt weder die Verarbeitung

noch weiterer personenbezogener Daten in diesem Zusammenhang noch führt sie automatisch zu einer ausdrücklichen Einwilligung im Sinne von Art. 9 Abs. 2 Bst. a DSGVO. Und schliesslich hielt der EuGH erneut fest, dass das grundsätzliche Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten aus Art. 9 Abs. 1 DSGVO unabhängig davon gilt, ob die Information richtig ist oder nicht und ob der Verantwortliche überhaupt die Absicht hatte, solche Datenkategorien zu erheben.

Dieses Urteil bietet insbesondere wertvolle Hinweise zur zulässigen Dauer der Datenverarbeitung zu Werbezwecken und ist daher von grosser Bedeutung für die Arbeit der DSS. Der Gerichtshof stellt klar, dass die Verarbeitung personenbezogener Daten strikt auf das absolut Notwendige im Hinblick auf den verfolgten Zweck beschränkt sein muss. Eine unbegrenzte Speicherung solcher Daten zu gezielten Werbezwecken betrachtet das Gericht als unverhältnismässigen Eingriff in die durch die DSGVO garantierten Rechte. Die DSS ist der Auffassung, dass diese Einschränkung nicht nur für Nutzer sozialer Netzwerke gilt, sondern auch für Personen, deren Daten im Rahmen des Adresshandels oder Direktmarketings genutzt werden.

«Die DSS war im Berichtsjahr stärker als in den Vorjahren in den eigentlichen Gesetzgebungsprozess integriert und konnte die zuständigen Amtsstellen bereits bei der Ausarbeitung der Gesetzesvorlagen umfassend beraten.»

3. Stellungnahmen zu Vorlagen und Erlassen

Die DSS begutachtete im Berichtsjahr insgesamt 26 Vorlagen und Erlasse. Dem Trend der letzten ein bis zwei Jahre folgend stellten sich zunehmend weniger datenschutzrechtliche Fragen in Bezug auf die Vorlagen. Dies ist zum einen dadurch bedingt, dass bereits 2018 die meisten Gesetze im Zuge der Totalrevision des DSG angepasst wurden und damals nicht erfolgte Korrekturen in den letzten Jahren vorgenommen wurden. Zum anderen war die DSS im Berichtsjahr stärker als in den Vorjahren in den eigentlichen Gesetzgebungsprozess integriert worden und konnte die zuständigen Amtsstellen bereits bei der Ausarbeitung der Gesetzesvorlagen umfassend beraten.

In Bezug auf den **Vernehmlassungsbericht der Regierung betreffend die Schaffung eines Gesetzes über die europäischen elektronischen Mautsysteme (Umsetzung der Richtlinie der (EU) 2019/520 über die Interoperabilität elektronischer Mautsysteme und die Erleichterung des grenzüberschreitenden Informationsaustauschs über die Nichtzahlung von Strassenbenutzungsgebühren in der Union)** traf die DSS folgende Feststellungen:

Nachdem es sich bei der zu regelnden Rechtsmaterie nicht um die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung durch die dafür zuständigen öffentlichen Stellen handelt, sind die Art. 45 ff. DSG nicht anwendbar. Korrekterweise muss sich das nationale Gesetz auf die DSGVO als die übergeordnete Rechtsvorschrift stützen.

In den Erläuterungen erfolgten zudem Ausführungen zum Zusammenhang zwischen der Löschung der Protokolldaten und dem Recht auf Auskunft. Diese Ausführungen sind zwar im Ergebnis korrekt, sie geben allerdings nur wieder, was aus der Natur der Sache bzw. der DSGVO sowieso folgt, nämlich dass eine Auskunft nur über vorhandene Daten möglich ist. Sobald Daten gelöscht werden, können sie naturgemäss nicht mehr Gegenstand einer Auskunft sein. Die DSS empfahl daher, auf diesen Satz zu verzichten.

Des Weiteren regte die DSS an, Art. 11 anders auszugestalten. Die gewählte Überschrift zu Art. 11 «Auskunftsrecht und Datenschutz» entsprach nicht dem nachfolgenden, sehr eng gehaltenen Gesetzesinhalt, der sich ausschliesslich auf den Zeitraum der Protokollierung und die danach zu erfolgende Löschung bezog. Die DSS empfahl daher, an Stelle von «Datenschutz und Auskunftsrecht» den Begriff «Datenverarbeitung» zu verwenden und dann zusätzlich in Art. 11 einen Absatz aufzunehmen, der die nationale Rechtsgrundlage für die rechtmässige Datenverarbeitung und -weiterleitung durch das Amt für Strassenverkehr (ASV) darstellt. Dabei können die rechtmässig verarbeiteten Daten sowie die Offenlegung an andere nationale Kontaktstellen spezifiziert werden. Im Grunde könnte auch Art. 10 Abs. 2 in diesen Artikel zur Datenverarbeitung integriert werden.

Die Formulierung des Art. 11 Abs. 1 liess zudem vermuten, dass das Auskunftsrecht nicht nur von natürlichen, sondern auch von juristischen Personen («Jeder von einem Datenabruf nach Art. 9 Abs. 2 betroffene Fahrzeugeigentümer oder -halter hat das Recht…») ausgeübt werden kann. Dies ist möglich, sollte aber zumindest in den Erläuterungen näher ausgeführt werden.

Ebenfalls stellte die DSS eine Diskrepanz in Bezug auf die Regelung des Auskunftsrechtes fest. In Art. 11 Abs. 1 hiess es, dass die Auskunft unverzüglich zu erteilen ist. Art. 12 Abs. 3 DSGVO sieht hingegen vor, dass die Auskunft «unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen ist». Sollte für den Anwendungsbereich dieses Gesetzes tatsächlich von der Frist eines Monats abgewichen werden wollen, wäre dies in den Erläuterungen zu begründen. Die DSS riet allerdings davon ab und empfahl an Stelle des Begriffs «unverzüglich» auf Art. 12 Abs. 3 DSGVO zu verweisen.

In Bezug auf **den Vernehmlassungsbericht der Regierung betreffend die Abänderung des Allgemeinen Bürgerlichen Gesetzbuches sowie weiterer Gesetze (Revision Sachwalterrecht)** wies die DSS auf die folgenden kritischen Punkte hin:

Der aktuelle Art. 126 des Ausserstreitgesetzes regelt die Verständigungspflichten. Dabei ist gemäss Abs. 1 ein begründetes Interesse für die Verständigung erforderlich, nach Abs. 2 erfolgt die Eintragung in öffentliche Bücher und Register, wenn der Wirkungskreis des Sachwalters die eingetragenen Rechte umfasst und nach Abs. 3 kann das Gericht Auskunft erteilen, wenn der Dritte ein rechtliches Interesse glaubhaft macht. Mit der vorliegenden Abänderung sollen die Gerichte neu gemäss Art. 126 Abs. 2 Ausserstreitgesetz verpflichtet werden, die Daten betreffend Sachwalterbestellungen jeweils auch im Zentralen Personenregister (ZPR) einzutragen.

Die DSS regte an, in diesem Zusammenhang Folgendes zu bedenken: Die Berechtigungen in Bezug auf Schreib- und Leserechte richten sich nach dem Gesetz

über das Zentrale Personenregister (ZPRG). Wenn somit einer öffentlichen Stelle Leserechte eingeräumt werden, muss diese kein spezifisches berechtigtes oder rechtliches Interesse geltend machen. Wenn die Informationen zu Sachwalterbestellungen für die Erfüllung ihrer öffentlichen Aufgaben erforderlich sind, kann das Leserecht gewährt werden. Die Frage der Erforderlichkeit ist somit a priori und generell zu beurteilen und kann recht weit verstanden werden. Art. 14 ZPRG ist nämlich vom Grundsatz so ausgestaltet, dass Berechtigungen vorab vergeben werden und nicht auf einen spezifischen Fall begrenzt sind. Auch wenn die Abfragen dann im Einzelfall zu begründen sind, ist dies aus Sicht des Datenschutzes eine Einschränkung der Rechte der betroffenen Personen, da der Zugriff ohne Einzelfallprüfung erfolgen kann und die Eingabe einer Begründung lediglich der nachträglichen Kontrolle dient. Eine solche nachträgliche Kontrolle erfolgt im Normalfall zudem nur in den seltensten Fällen und ist daher mit einer inhaltlichen Vorabprüfung nicht zu vergleichen.

«Die bereits in den Vorjahren etablierte enge Zusammenarbeit zwischen Technik und Recht erwies sich auch im Berichtsjahr als essenziell für zahlreiche Aufgabenbereiche.»

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

Die DSS konnte trotz der hohen Anforderungen mit dem bestehenden Personalbestand von 700 Stellenprozenten ihre Aufgaben im Berichtsjahr erfolgreich erfüllen. Erfreulicherweise ergab sich die Möglichkeit, eine Juristenstelle, die aufgrund einer Pensionierung im Sommer 2025 vakant wird, bereits im November des Berichtsjahres nachzubesetzen. Dies ermöglicht eine reibungslose Übergabe und gewährleistet die Kontinuität der juristischen Expertise innerhalb der Organisation.

Die bereits in den Vorjahren etablierte enge Zusammenarbeit zwischen Technik und Recht erwies sich auch im Berichtsjahr als essenziell für zahlreiche Aufgabenbereiche. Besonders die Frage der Rechtskonformität von Webanalyse- oder Einwilligungsmanagement-Tools und vergleichbaren Technologien war auch 2024 wieder kontinuierlich präsent und erforderte eine tiefgehende Auseinandersetzung mit technischen sowie rechtlichen Aspekten. Die zunehmende Dynamik neuer Technologien machte es zudem erforderlich, das technische Verständnis innerhalb der DSS kontinuierlich zu vertiefen, um fundierte Bewertungen und praxisnahe Lösungen sicherzustellen.

Darüber hinaus wurde deutlich, dass die interdisziplinäre Zusammenarbeit in Zukunft weiter ausgebaut werden muss, um den sich stetig wandelnden regulatorischen und technologischen Anforderungen gerecht zu werden. Die zunehmende Komplexität der Datenschutzfragen erfordert nicht nur eine rechtliche, sondern auch eine technische Expertise, die in Entscheidungsprozesse frühzeitig eingebunden werden sollte.

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 zwei Fällen je einen Experten zwecks Evaluierung eines anderen Schengen-Staates.

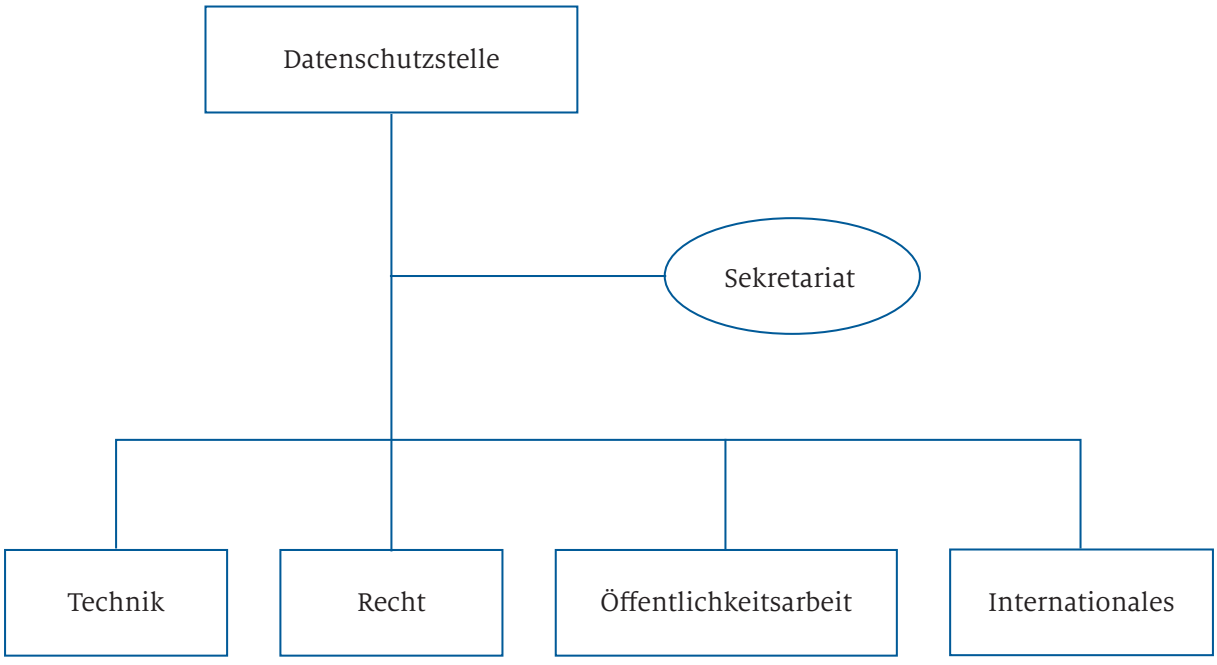


Abbildung 3: Organigramm Datenschutzstelle

«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 der Datenschutz-Aufsichtsbehörden 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 im Kapitel «Wichtigste EuGH-Entscheidungen 2024» zur Rechtssache «EuGH, 26. September 2024, C-768/21: TR v. Land Hessen (Entscheidungsspielraum der Aufsichtsbehörde)» dargelegt, hält die DSS klar an der Auffassung fest, dass ihre Unabhängigkeit und Autonomie voraussetzen, dass sie eigenständig über die zu ergreifenden Abhilfemassnahmen und Sanktionen entscheidet. Nur so kann sichergestellt werden, dass ihre Entscheidungen frei von politischem oder wirtschaftlichem Einfluss getroffen werden und die Durchsetzung des Datenschutzrechts nicht von externen Interessen beeinträchtigt wird.

Mit dem EuGH-Urteil vom September 2024 wurde dieser Grundsatz nun auch höchstgerichtlich bestätigt. Das Urteil bekräftigt, dass Datenschutz-Aufsichtsbehörden nicht nur formal unabhängig sein müssen, sondern auch inhaltlich und operativ über die volle Entscheidungsfreiheit verfügen, um eine wirksame und objektive Aufsicht zu gewährleisten. Dies unterstreicht die zentrale Rolle der Aufsichtsbehörden als unabhängige Hüter der Datenschutzgrundrechte und sichert ihre Fähigkeit, Verstösse effektiv und ohne äusseren Druck zu sanktionieren.

Entgegen anderweitiger Planung musste die DSS jedoch auch im Berichtsjahr erneut feststellen, dass die aktuellen Personalressourcen für umfassende amtswegige Überprüfungen bei Unternehmen nicht ausreichen. Folglich wurde erneut entschieden, amtswegige Überprüfungen nur dann durchzuführen, wenn die DSS 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 öffentlichen Organisationen spezifische Untersuchungen aufgrund von konkreten Anlassfällen durchgeführt. Dabei wurde jeweils Hinweisen oder Anzeichen dafür nachgegangen, dass bei den Organisationen unzulässige Datenverarbeitungen stattgefunden haben. Daneben wurden auch zahlreiche Überprüfungen von Videoüberwachungsanlagen Privater durchgeführt und eine Videoüberwachungsanlage der Landespolizei von Amtes wegen kontrolliert.

Darüber hinaus eröffnete die DSS im Berichtsjahr von Gesetzes wegen je eine datenschutzrechtliche Überprüfung des Einsatzes der europäischen IT-Systeme der Landespolizei (SIS) sowie des Ausländer- und Passamts (VIS).

Schliesslich entsandte die DSS 2024 im Rahmen der Mitgliedschaft Liechtensteins im Schengen-Raum auch wieder je einen Experten an zwei der regelmässig durchzuführenden Länder-Überprüfungen.

5.1.1 Amtswegige Überprüfungen bei Unternehmen

Nachfolgend werden zwei Beispiele der im Berichtsjahr vorgenommenen amtswegigen Datenschutzüberprüfungen der DSS bei Unternehmen vorgestellt.

Amtswegige Überprüfung bei einem Zustellunternehmen

Im Berichtsjahr wurde eine datenschutzrechtliche Prüfung bei einem Zustellunternehmen eingeleitet, das in seinen Fahrzeugen Telematiksysteme einsetzt. Diese Systeme dienen dazu, die Zustellqualität gegenüber Auftraggebern nachzuweisen und unberechtigte Reklamationen abzuwehren. Ziel der Kontrolle war die Überprüfung, ob die rechtliche, technische und

organisatorische Umsetzung der Datenverarbeitung im Zusammenhang mit dem Telematiksystem den datenschutzrechtlichen Anforderungen im Hinblick auf die Mitarbeitenden entspricht. Die Prüfung wurde zunächst als Dokumentenanalyse durchgeführt, ohne eine Vor-Ort-Kontrolle vorzunehmen. Zum Ende des Berichtsjahres war die Datenschutzkontrolle jedoch noch nicht abgeschlossen und die Prüfung der datenschutzkonformen Gestaltung der eingesetzten Telematiklösungen weiterhin im Gange.

Amtswegige Überprüfung bei einem Sportveranstalter

Im Berichtsjahr erhielt die DSS einen Hinweis auf möglicherweise problematische Datenschutzverarbeitungen im Zusammenhang mit einer gross angelegten Sportveranstaltung in Liechtenstein. Aufgrund der hohen Anzahl potenziell betroffener Personen wurde eine Datenschutzüberprüfung eingeleitet, die sich insbesondere auf die Verarbeitung von Bild- und Videoaufnahmen sowie die personenbezogenen Daten der Teilnehmenden konzentrierte.

Die erfassten Bild- und Videoaufnahmen wurden teilweise von der verantwortlichen Stelle selbst erstellt und verfolgten sowohl dokumentarische als auch marketingbezogene Zwecke. Die verantwortliche Stelle berief sich hierfür auf ihr berechtigtes Interesse sowie in bestimmten Fällen auf die Einwilligung der betroffenen Personen. Die DSS stellte fest, dass das berechtigte Interesse eine mögliche rechtliche Grundlage für Dokumentationszwecke sein kann. Für Marketingzwecke ist dies jedoch nicht zulässig, da Teilnehmende nicht automatisch damit rechnen müssen, dass ihre Aufnahmen kommerziell verwendet werden. In diesen Fällen ist eine informierte, freiwillige und klar dokumentierte Einwilligung erforderlich, um die Datenschutzvorgaben einzuhalten.

Zusätzlich wurden Aufnahmen von einem ausländischen Fotografenteam angefertigt, das auf Sportveranstaltungen spezialisiert ist. Im Rahmen der Untersuchung stellte die DSS fest, dass dieses Fotografenteam als eigenständiger Verantwortlicher im Sinne der DSGVO für die Verarbeitung der Aufnahmen einzustufen war. Da sich in Bezug auf die Datenverarbeitung durch das Fotografenteam zahlreiche kritische Fragen ergaben, übermittelte die DSS diese an die zuständige ausländische Datenschutzbehörde, die daraufhin die weitere Untersuchung übernahm.

Darüber hinaus stellte die DSS fest, dass die Informationspflichten gemäss Art. 13 DSGVO nicht ausreichend erfüllt wurden – sowohl bei der Datenverarbeitung durch die verantwortliche Stelle als auch durch das externe Fotografenteam. Die betroffenen Personen erhielten keine hinreichende Aufklärung über die Verarbeitung ihrer Daten. Zudem fehlte für die Verarbeitung bestimmter Daten der Teilnehmenden eine klare rechtliche Grundlage, was zu rechtlichen Unsicherheiten führte. Ein weiteres Problem war die unzureichende Datenlöschung: Daten wurden über die erforderliche Dauer hinaus gespeichert, da kein geeignetes Löschkonzept implementiert war.

Im Anschluss an die Überprüfung führte die DSS eine Beratung mit der verantwortlichen Stelle durch. Dabei wurden wesentliche Datenschutzaspekte erörtert, insbesondere die Anforderungen an eine rechtskonforme Verarbeitung und Speicherung von personenbezogenen Daten. Zudem wurde die Datenschutzerklärung der Veranstaltung gemeinsam mit der DSS überarbeitet, um den Datenschutzanforderungen besser gerecht zu werden.

5.1.2 Amtswegige Überprüfung bei öffentlichen Stellen

Genau 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 hat die DSS auch beim Amt für Tiefbau und Geoinformation eine bestimmte Datenverarbeitung überprüft.

Amtswegige Überprüfung beim Amt für Tiefbau und Geoinformation

Im Berichtsjahr wandten sich die Verantwortlichen des Amtes für Tiefbau und Geoinformation (ATG) an die DSS mit einer Beratungsanfrage zur Nutzung von Fahrzeug-Telematik in ihren Werksfahrzeugen. Fast zeitgleich erhielt die DSS eine Beschwerde über den Einsatz dieser GPS-Tracker, was zur Einleitung einer amtswegigen Untersuchung führte. Im Zentrum der Prüfung standen die Rechtsgrundlage und der Verwendungszweck der GPS-Datenverarbeitung.

Die DSS kam zum Schluss, dass bei der datenschutzrechtlichen Beurteilung eine Unterscheidung zwischen Werksdienstfahrzeugen und Winterdienstfahrzeugen erforderlich ist:

- Werksdienstfahrzeuge: Für die Nutzung von GPS-Trackern in diesen Fahrzeugen konnte keine ausreichende Rechtsgrundlage festgestellt werden, weshalb die Datenverarbeitung als unzulässig eingestuft wurde.
- Winterdienstfahrzeuge: Hier konnte eine gesetzliche Grundlage im Baugesetz und im Allgemeinen bürgerlichen Gesetzbuch identifiziert werden. Allerdings sind für eine abschliessende

Bewertung der Zulässigkeit noch weitere rechtliche und praktische Abklärungen erforderlich.

Aus datenschutzrechtlicher Sicht ist der Einsatz von GPS-Tracking besonders kritisch, da er einen tiefgreifenden Eingriff in die Privatsphäre der Mitarbeitenden darstellt. Eine ständige Erfassung von deren Aufenthaltsort kann zu einem erheblichen Überwachungsdruck führen und das Vertrauensverhältnis zwischen Arbeitgeber und Beschäftigten stark beeinträchtigen. Daher muss eine solche Massnahme rechtlich gut begründet und verhältnismässig sein, insbesondere wenn sie im Arbeitsalltag flächendeckend eingesetzt wird.

Die noch offenen Fragen werden im Folgejahr gemeinsam mit dem ATG im Detail erörtert, um sicherzustellen, dass die GPS-Datenverarbeitung den datenschutzrechtlichen Anforderungen entspricht.

5.1.3 Aufsicht über Videoüberwachungsanlagen

Die Abgrenzung zwischen Beratung und Beschwerde im Bereich der Videoüberwachung gestaltet sich häufig schwierig, insbesondere weil Betroffene oft unsicher sind, ob sie eine formelle Beschwerde einreichen möchten. Um diesen Unsicherheiten entgegenzukommen, akzeptiert die DSS auch informelle Beschwerden, insbesondere bei Überwachungen im nachbarschaftlichen Umfeld. Ziel ist es, zunächst eine einvernehmliche Lösung zwischen den Parteien zu finden, bevor eine formelle Prüfung eingeleitet wird.

Nachbarschaftliche Videoüberwachungen sind eine häufige Quelle von Konflikten, sei es aufgrund der Überwachung selbst oder als Folge bereits bestehender Streitigkeiten. Unabhängig vom konkreten Kontext nimmt die DSS solche Anliegen sehr ernst und bewertet die Sachlage objektiv aus datenschutzrechtlicher Sicht. Grundsätzlich ist die Überwachung privater Wohnflächen und Grundstücke erlaubt, solange keine weiteren Personen betroffen sind und die Überwachung ausschliesslich auf das eigene Grundstück beschränkt bleibt. Allerdings kann selbst eine formal zulässige Überwachung problematisch sein, wenn sie zu einem subjektiven Überwachungsdruck für Nachbarn, Anwohner oder Passanten führt.

Da ein solcher Überwachungsdruck in der Regel in den Bereich des Personen- und Gesellschaftsrechts (PGR) fällt, ist die DSS hierfür nicht direkt zuständig. Im Rahmen ihrer Beratungen informiert sie jedoch regelmässig über rechtliche Möglichkeiten, die in solchen Fällen bestehen.

Im Berichtsjahr konnten alle eingegangenen Fälle durch Vor-Ort-Begehungen und Gespräche mit den Beteiligten geklärt werden. Eine formell eingereichte Beschwerde musste zurückgewiesen werden, da sie nicht von der betroffenen Person selbst, sondern stellvertretend durch eine dritte Partei eingereicht wurde. Damit die DSS auf eine Beschwerde eintreten kann, muss der Beschwerdeführer entweder selbst betroffen sein, ein gesetzlicher Vertreter sein oder über eine entsprechende Vollmacht verfügen. Trotz mehrmaliger Nachfragen wurde diese Vollmacht nicht nachgereicht, wes-

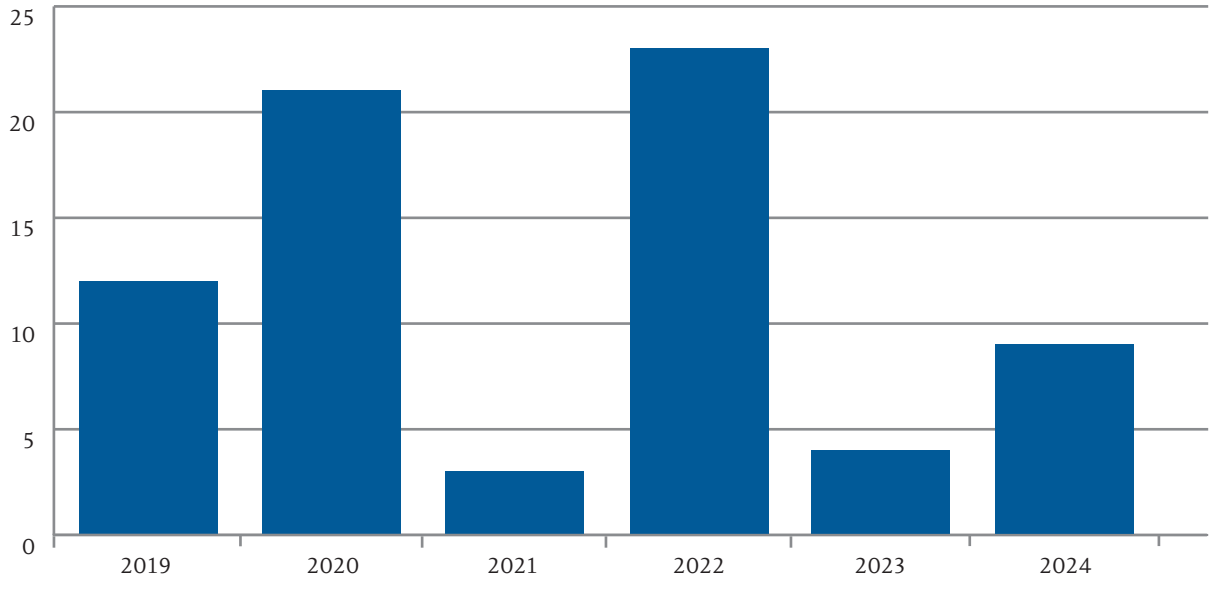


Abbildung 4: Anzahl der Datenschutzüberprüfungen pro Jahr (ohne Videoüberwachungen)

halb die Beschwerde nicht weiterbearbeitet werden konnte.

5.1.4 Überprüfungen von Gesetzes wegen

Die DSS eröffnete im Berichtsjahr von Gesetzes wegen je eine datenschutzrechtliche Überprüfung des Einsatzes der europäischen IT-Systeme der Landespolizei (SIS) sowie des Ausländer- und Passamtes (VIS). Regelmässige Überprüfungen des Einsatzes dieser Systeme sind vom Schengen-Acquis gesetzlich gefordert und richten sich nach internationalen Prüfungsstandards. Der Fokus der DSS liegt dabei insbesondere auf technischen und organisatorischen Massnahmen wie Zugriffsbeschränkungen, Speicherdauer und Datensicherheit, aber auch auf den Informationspflichten nach DSGVO und DSG wie auch rechtlichen Aspekten. In Zusammenhang mit der im Berichtsjahr angestossenen Überprüfung stellten sich insbesondere spannende Fragen bezüglich neuer Fahndungsmöglichkeiten und deren nationaler Handhabung.

5.1.5 Schengen-Evaluationen im In- und Ausland

Im Rahmen der regelmässigen Schengen-Evaluationen entsandte die DSS im Februar einen Juristen nach Kroatien und im April einen IT-Experten nach Polen. Die DSS nimmt ausserdem regelmässig an den Sitzungen des Coordinated Supervision Committee (CSC) teil. Das CSC besteht aus Mitarbeitenden der nationalen Aufsichtsbehörden und des Europäischen Datenschutzbeauftragten (EDSB) und hat die Aufgabe, eine koordinierte Aufsicht über IT-Grosssysteme und Einrichtungen, Ämter und Agenturen der EU gemäss Art. 62 der Verordnung (EU) 2018/1725 oder dem EU-Rechtsakt zur Einrichtung des IT-Grosssystems oder der Einrichtung, des Amtes oder der Agentur der EU sicherzustellen. Im Berichtsjahr wurden vier Sitzungen abgehalten. Zusätzlich zu den bereits integrierten acht IT-Gross-Systemen der EU (u.a. Schengen Information System (SIS), Internal Market Information System (IMI), European Union Agency for Law Enforcement Cooperation (Europol) und Visa Information System (VIS)) werden in naher Zukunft weitere IT-Gross-Systeme wie beispielsweise das Entry/Exit System (EES), das European Travel Information and Authorisation System (ETIAS) oder auch die European Asylum Dactyloscopy Database (EURODAC) unter die datenschutzrechtliche Aufsicht des CSC gestellt werden.

Liechtenstein selbst wird im Jahr 2026 durch externe Experten, bestehend aus Mitarbeitenden der 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, bei der Landespolizei sowie dem SIRENE-Büro. Weitere Vorbereitungen für die externe Schengen-Evaluation sind für das Jahr 2025 vorgesehen.

5.2 Beschwerden

Betroffene Personen haben nach Art. 77 DSGVO das Recht, sich bei der Aufsichtsbehörde zu beschwe-

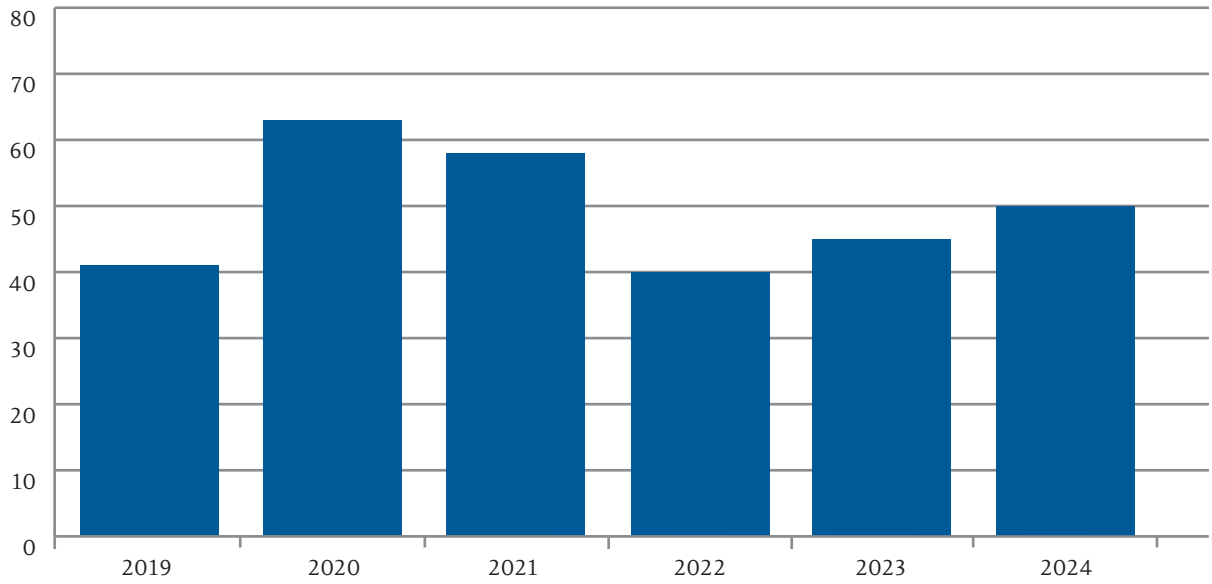


Abbildung 5: Anzahl der Beschwerden pro Jahr

ren, 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 gingen bei der DSS im Berichtsjahr 50 Beschwerden und somit rund 11% mehr als im Vorjahr ein.

5.2.1 Nationale Beschwerden

Im Berichtsjahr erhielt die DSS insgesamt 48 Beschwerden von Privatpersonen, die sich direkt an die DSS als für ein liechtensteinisches Unternehmen oder eine öffentliche Stelle zuständige Behörde richteten. Die Beschwerdeführer haben zum überwiegenden Teil ihren Wohnsitz in Liechtenstein. Aber auch Personen aus dem EWR, vor allem Deutschland, brachten Beschwerden 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 Geldbussen über insgesamt CHF 21'500 wurden im Berichtsjahr für drei gravierende Verstösse verhängt, in zwei Fällen wegen Nicht-Umsetzung von bereits mit vorgängiger Verfügung der DSS angeordneten Massnahmen, in einem Fall insbesondere wegen mangelhaften Sicherheitsvorkehrungen (entgegen einer früheren Beratung durch die DSS) und der daraus folgenden fahrlässigen Offenlegung von Gesundheitsdaten. Nachdem in all diesen Fällen bereits mehrfache Verwarnungen durch die DSS ausgesprochen worden waren, scheiterte die Verhängung des Bussgeldes nicht an der Formulierung des Art. 40 Abs. 6 DSG, welcher eine vorgängige Verwarnung erforderlich macht.

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 einige langwierige und aufwändige Verfahren verhindert werden.

5.2.2 Internationale Beschwerden

Art. 56 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 Verarbeitung 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 Datenschutzbehörden von Personen aus einem anderen EWR-Staat, die sich gegen ein liechtensteinisches Unternehmen richteten. Umgekehrt wurde im Berichtsjahr keine Beschwerde von einer Person aus Liechtenstein an eine andere europäische Datenschutzbehörde weitergeleitet.

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:

Unter welchen Voraussetzungen kann sich ein Verantwortlicher auf Art. 34 DSG stützen?

Die verantwortliche Stelle machte geltend, dass sie bei der Erteilung der Auskunft gemäss Art. 15 DSGVO von der in Art. 34 Abs. 1 Bst. b Ziff. 2 DSG vorgesehenen Ausnahme Gebrauch gemacht hätte. Gemäss diesem Gesetzesartikel kann von einer Auskunftserteilung abgesehen werden, wenn die Datenverarbeitungen «ausschliesslich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und die Auskunftserteilung einen unverhältnismässigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Massnahmen ausgeschlossen ist.» Konkret ging es um E-Mails von anderen Mitarbeitenden, die einzelne personenbezogene Daten des Beschwerdeführers zum Inhalt hatten.

Die DSS führte in ihrer rechtlichen Beurteilung Folgendes aus: Im Rahmen einer E-Mail Archivierung ist grundsätzlich jedes Dokument zum organisatorisch frühestmöglichen Zeitpunkt zu archivieren. Die Archivierung dient der Umsetzung der Grundsätze in Art. 5 Abs. 1 DSGVO, insbesondere der Datenminimierung, Zweckbestimmung sowie der Vertraulichkeit

und Integrität. Die DSS ging zudem davon aus, dass die Archivierung zu einem angemessenen Zeitpunkt stattfand. Gemäss Vorbringen der verantwortlichen Stelle bezog sich der Inhalt der fraglichen E-Mails lediglich auf eine Information, aus der vernünftigerweise geschlossen werden konnte, dass diese E-Mails keine materiell bedeutsame Relevanz für ein Kundendossier hatten, und folglich auch nicht weiterhin für eine aktive Bearbeitung des Dossiers von Relevanz waren. Somit war es auch auf den Inhalt bezogen für die DSS plausibel, E-Mails mit derartigem Inhalt in das Archiv zu verschieben, wo sie nur mehr zum Zweck der Datensicherung oder einer Datenschutzkontrolle vorhanden waren.

Die Verwendung eines automatisierten Archivierungssystems, das ausschliesslich der Datensicherung dient, ist folglich als rechtmässig und unter Art. 34 DSG subsumierbar zu qualifizieren. Ebenso ist es plausibel, dass das Auffinden einzelner E-Mails im Archiv, bei denen nur der Name des Beschwerdeführers irgendwo im Inhalt der E-Mails enthalten ist, mit unverhältnismässigem Aufwand verbunden ist. Schliesslich war davon auszugehen, dass das Archiv mit adäquaten technischen und organisatorischen Massnahmen vor einer anderweitigen Verarbeitung geschützt ist, da der Zugriff auf nur mehr wenige Personen eingeschränkt ist.

Selbst wenn somit die Beschränkung der Auskunft nach Art. 15 DSGVO unter Berufung auf Art. 34 Abs. 1 Bst. b Ziff. 2 DSG aus Sicht der DSS gerechtfertigt ist, wäre die verantwortliche Stelle aber verpflichtet gewesen, die betroffene Person im Rahmen der Auskunft darüber zu informieren. Dies wird konkret von Art. 34 Abs. 2 DSG verlangt, wonach «Die Ablehnung der Auskunftserteilung gegenüber der betroffenen Person zu begründen ist, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.» Insoweit war eine Verletzung des Auskunftsrechts des Beschwerdeführers festzustellen, denn die verantwortliche Stelle hätte im Auskunftsschreiben darauf hinweisen müssen, dass es zumindest möglich ist, dass sie weitere personenbezogene Daten des Beschwerdeführers ausschliesslich zu Datensicherungszwecken verarbeitet und sie diesbezüglich von der in Art. 34 Abs. 1 DSG vorgesehenen Ausnahme Gebrauch macht.

Beschwerde betreffend eine angebliche Datenzusammenführung durch das Amt für Gesundheit (AG)

Eine betroffene Person hatte ein Auskunftsgesuch gemäss Art. 15 DSGVO an das AG gestellt. Die betroffene Person präzisierte ihre Beschwerde im weiteren Verfahren dahingehend, dass ihr Auskunftsbegehren ausschliesslich auf die Verarbeitung ihrer Daten im elektronischen Gesundheitsdossier (eGD) abzielte und sie nur in Bezug auf das eGD eine Auskunft verlangt hatte. Stattdessen erhielt sie vom AG eine Auskunft zu sämtlichen zu ihrer Person verarbeiteten Daten. Daraus schloss sie, dass mehr Daten in ihrem eGD gespeichert würden als bei einem Widerspruch rechtlich erlaubt wäre. Die DSS gab der Beschwerdeführerin insofern recht, als das AG seine Auskunftserteilung auf das klar eingeschränkte Auskunftsgesuch hätte begrenzen können. Die zu beantwortende Rechtsfrage betraf somit die Frage, ob ein «Zuviel» der Auskunft als Verstoss gegen Art. 15 DSGVO zu werten ist.

Die DSS verneinte diese Frage und begründete dies wie folgt: Aus dem Wortlaut des Art. 15 DSGVO folgt, dass sich das Auskunftsrecht grundsätzlich auf sämtliche personenbezogene Daten bezieht, die von einem Verantwortlichen zu einer betroffenen Person verarbeitet werden. Dies wird auch durch ErwG 63 bestätigt, der es dem Verantwortlichen zugesteht, dass er die betroffene Person ersucht, das Auskunftsgesuch zu begrenzen, wenn es sich insgesamt um eine sehr grosse Datenmenge handelt. Wenn nun eine verantwortliche Stelle mehr Daten beauskunftet als von der betroffenen Person verlangt, kann dies nicht als Verletzung des Art. 15 DSGVO gewertet werden. Vor allem dann nicht, wenn in der Auskunft in verständlicher und transparenter Weise unterschieden wird zwischen der Verarbeitung von Daten in Bezug auf das konkrete Auskunftsgesuch, somit hier das eGD, unter der Überschrift A und weiteren Datenverarbeitungen durch das AG unter den Überschriften B und C.

Durch die klare Unterteilung in drei Bereiche und auch die Kopien, die diesen drei Bereichen zugeordnet werden können, kann keine Schlussfolgerung gezogen werden, dass es Verknüpfungen oder Schnittstellen zwischen den drei Bereichen gibt. Wie im Auskunftsschreiben ausgeführt, ist jeder Bereich einer getrennten Rechtsgrundlage für die Datenverarbeitung zugeordnet und gerade die Kopie des eGD zeigt, dass dieses tatsächlich keinen Inhalt aufweist.

Beschwerde betreffend die Weitergabe von Gesundheitsdaten eines Gesundheitsdienstleisters an weitere Empfänger

Eine betroffene Person brachte in ihrer Beschwerde vor, dass während der Covid 19-Pandemie Gesundheitsdaten von einem Gesundheitsdienstleister an weitere Empfänger unrechtmässig weitergeleitet wurden. Sie sah die Berufung der verantwortlichen Stel-

le auf Art. 9 Abs. 2 Bst. i DSGVO, wonach die Verarbeitung besonderer Kategorien personenbezogener Daten erlaubt ist, wenn diese «aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren» erforderlich ist, als nicht ausreichend an.

Die DSS gab der Beschwerde recht. Zwar dient Art. 9 Abs. 2 Bst. i DSGVO dem Zweck der öffentlichen Gesundheit und dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, aber er verlangt ganz klar eine nationale Rechtsgrundlage, welche die Empfänger definiert. Im gegebenen Fall war die nationale Rechtsgrundlage das schweizerische Epidemiengesetz (EpG), gestützt auf den Zollanschlussvertrag zwischen der Schweiz und Liechtenstein vom 29. März 1923, LGBl. 1923/24, sowie die Verordnung vom 17. Februar 2022 über Massnahmen zur Bekämpfung des Coronavirus (Covid-19), LGBl. 2022/18. In beiden Rechtsakten sind die Empfänger der Daten jedoch abschliessend aufgelistet, sodass die Liste nur über eine Abänderung des Gesetzes oder der Verordnung hätte erweitert werden können, um auch die fragliche Datenweiterleitung zu umfassen.

Darüber hinaus ist zu berücksichtigen, dass Art. 9 Abs. 2 Bst. i DSGVO die «Erforderlichkeit» als ausschlaggebendes Kriterium festschreibt. Für eine Erweiterung der Empfänger hätte somit auch das Kriterium der Erforderlichkeit für den genannten Zweck erfüllt sein müssen.

5.2.4 Entscheidungen der Beschwerdekommission für Verwaltungsangelegenheiten (VBK)

Im Berichtsjahr entschied die VBK über fünf Beschwerden, welche von einer der beiden Verfahrensparteien gegen Verfügungen der DSS eingebracht worden waren. In drei Fällen bestätigte die VBK die Entscheidungen der DSS; in zwei Fällen wurde die Beschwerde verworfen. Eine Beschwerde ist nach wie vor bei der VBK hängig.

5.2.5 Beschwerden an den Verwaltungsgerichtshof (VGH)

Im Berichtsjahr wurde in zwei ursprünglich bei der DSS eingebrachten Beschwerdefällen Beschwerde an den VGH erhoben, nachdem die VBK die Entscheidungen der DSS bestätigt hatte. Beide betreffen einen identen Sachverhalt und waren am Ende des Berichtsjahrs beim VGH noch hängig.

Des Weiteren brachte eine öffentliche Stelle gegen eine von der VBK bestätigte Entscheidung der DSS Beschwerde beim VGH ein, zog diese dann aber wieder zurück.

5.2.6 Beschwerden an den Staatsgerichtshof (StGH)

Im Falle der vom VGH im Vorjahr entschiedenen Beschwerde betreffend eine Verfügung der DSS zur Geltendmachung des Berichtigungsrechts nach Art. 16 DSGVO erhob die Beschwerdeführerin Individualbeschwerde an den StGH. Der StGH gab dieser im Berichtsjahr keine Folge.

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.

Im Berichtsjahr erhielt die DSS 57 Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO, wobei in bislang abgeschlossenen Verfahren in 17 Fällen die betroffenen Personen benachrichtigt wurden (Art. 34 DSGVO). Dies entspricht in etwa der Anzahl Meldungen und Benachrichtigungen im Vorjahr.

Auch in diesem Jahr stellte die Frage der Einschätzung des Risikos für die betroffenen Personen und somit der Benachrichtigungspflicht des Verantwortlichen jedoch eine Schwierigkeit dar, die einen umfangreichen Beratungsaufwand seitens der DSS erforderte.

Insgesamt zeigten die Meldungen im Berichtsjahr, dass es für die Verantwortlichen nicht immer einfach war, innerhalb der 72-Stunden-Frist alle relevanten Informationen im Unternehmen zusammenzutragen und beizubringen. Vielfach mussten daher fehlende Informationen zu einem späteren Zeitpunkt nachgeliefert werden. Die Meldungen erfolgten am häufigsten von Versicherungen und weiteren Finanzintermediären, dem Gewerbe, der Industrie und von IT-Dienstleistern.

Inhaltlich betrafen drei Viertel der Meldungen (74%) den irrtümlichen Versand von E-Mails an unberechtigte Empfänger, die versehentliche Veröffentlichung sensibler Daten auf öffentlich zugänglichen Plattformen sowie fehlerhafte Datenweitergaben durch menschliches Versagen. Nicht selten waren wiederum einfachste und bereits seit langem bekann-

te Sicherheitsmängel bzw. -fehler oder auch Systemupdates und Softwarefehler der Grund für die Datenpannen, weshalb auch für das Berichtsjahr davon auszugehen ist, dass die Dunkelziffer der tatsächlich erfolgten Vorfälle noch um einiges höher ist.

Von den übrigen gemeldeten Datenschutzverletzungen durch einen Hackerangriff fanden nur drei in Liechtenstein statt (5%). Die weiteren gemeldeten Vorfälle (21%) geschahen bei Verantwortlichen oder Auftragsverarbeitern im Ausland, insbesondere in der Schweiz, und betrafen keine oder nur wenige Personen in Liechtenstein. Häufig handelte es sich dabei nur um vorsorgliche Meldungen für den Fall, dass sich im Laufe der Untersuchung herausstellen sollte, dass auch Personen in Liechtenstein betroffen sind.

Die gemeldeten Vorfälle verdeutlichen die Notwendigkeit für datenverarbeitende Stellen, stets adäquate technische und organisatorische Massnahmen wie insbesondere regelmässige Sicherheitsüberprüfungen, die Verschlüsselung sensibler Daten, den Einsatz von Monitoring-Systemen sowie Zwei-Faktor-Authentifizierungen oder auch eines Berechtigungskonzepts umzusetzen, um das Risiko einer Datenschutzverletzung zu minimieren und ihr Ausmass zu begrenzen.

Die DSS möchte an dieser Stelle noch auf einen speziellen Fall bei der Einschätzung des Risikos für die Rechte und Freiheiten der betroffenen Personen von einer Datenschutzverletzung hinweisen. So gibt es Konstellationen, wo die während eines Vorfalls an Unberechtigte offengelegten Informationen keine besonders sensiblen Daten darstellen (z.B. E-Mail-Adressen) und deshalb zunächst nicht von einem hohen Risiko für die Betroffenen auszugehen ist. Wenn aber diese Daten bereits für kriminelle Zwecke wie etwa einen Betrugsversuch mittels Phishing-Mail verwendet wurden, so ist das Risiko für die Betroffenen in jedem Fall als hoch einzuschätzen und diese sind gemäss Art. 34 DSGVO unverzüglich über den Vorfall und das Phishing-Mail zu benachrichtigen. Nur so werden die betroffenen Personen in die Lage versetzt, entsprechende E-Mails zu ignorieren und zu löschen oder sonst rechtzeitig Massnahmen wie Passwortänderungen, die Sperrung von Konten oder die Implementierung weiterer Schutzvorkehrungen zu ergreifen, um potenziellen Schaden zu verhindern.

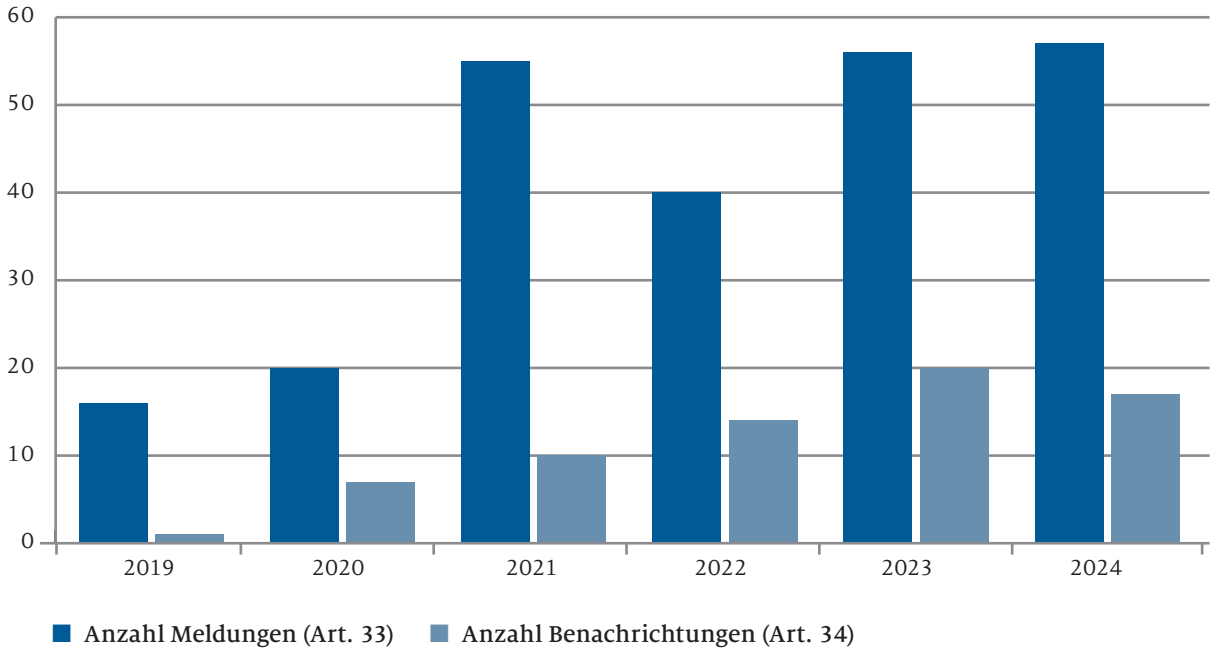


Abbildung 6: Anzahl der gemeldeten Datenschutzverletzungen pro Jahr

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

6. Mitarbeit in Arbeitsgruppen, Projekten und Kommissionen der Landesverwaltung

6.1 Modern Workplace

Im Berichtsjahr 2024 tagte der Fachausschuss des Projekts Modern Workplace viermal. Der Projektleiter informierte über Projektfortschritt und Anpassungen des Projektplans. In diesem Zusammenhang aktualisierte die DSS ihren Beitrag im Dokument «Microsoft Online Services – Grundlageninformation zu Informationssicherheit und Datenschutz».

6.2 Vorratsdatenspeicherung

Im Tätigkeitsbericht 2023 berichtete die DSS über ihre Beteiligung in der Arbeitsgruppe zur Vorratsdatenspeicherung und das hierbei aus Sicht des Datenschutzes erzielte positive Ergebnis, welches sicherstellen sollte, dass Strafverfolgungsbehörden ihre Arbeit weiterhin adäquat erledigen können, ohne dass die Bürgerinnen und Bürger einem unverhältnismässigen Eingriff in ihre Grundrechte ausgesetzt sind. Ende 2023 ging die Gesetzesrevision in die Vernehmlassung. Im Berichtsjahr gingen Rückmeldungen und Kommentare dazu ein. Diese führten zu weiteren intensiven Diskussionen innerhalb der Arbeitsgruppe, aber auch mit Telekommunikationsdienstanbietern und Schweizer Behörden wie dem Dienst «Überwachung Post- und Fernmeldeverkehr» (ÜPF).

Schliesslich musste bedauerlicherweise festgestellt werden, dass eine alleinige EuGH-konforme Anpassung der Vorratsdatenspeicherung durch den liechtensteinischen Gesetzgeber in der Praxis nicht durchführbar ist, ohne dass zeitgleich auch die schweizerische Gesetzgebung angepasst wird. Da in der Schweiz das Bundesgericht die aktuell geltende Vorratsdatenspeicherung – anders als der EuGH – für zulässig befunden hatte, ist nun auf ein entsprechendes Urteil des Europäischen Gerichtshofs für Menschenrechte in Strassburg zu warten. Die Arbeitsgruppe hat die Regierung dahingehend informiert und die weitere Bearbeitung der Gesetzesrevision wurde daher vorläufig ausgesetzt.

6.3 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, eine Abänderung im AIA-Gesetz sowie ein neues Abkommen zur fürsorgerischen Unterbringung.

6.4 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-Kommission obliegt die Entscheidung über die Offenlegungsanträge Dritter im Sinne von Art. 17 VwbPG. Im Berichtsjahr wurden zwei Anträge gemäss Art. 17 VwbPG betreffend die Offenlegung von Daten an Dritte an das Amt für Justiz gestellt. Ein Antrag wurde von der VwbP-Kommission im Berichtsjahr entschieden.

«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 2024 an den meisten Sitzungen der Arbeitsgruppen teilnehmen und aktiv mitarbeiten. Die DSS nahm ausserdem an zehn von zwölf Plenarsitzungen des Ausschusses teil.

7.1.1 Stellungnahmen, Leitlinien und Empfehlungen des EDSA

Der EDSA hat im Jahr 2024 auf Grundlage des Art. 64 Abs. 1 und 2 DSGVO insgesamt **28 Stellungnahmen** zu Vorlagen und Fragen von nationalen Datenschutz-Aufsichtsbehörden abgegeben. Darunter fielen:

- eine Stellungnahme zu bestimmten Datenschutzaspekten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen von KI-Modellen (Irland);
- eine Stellungnahme zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben (Dänemark);
- eine Stellungnahme zum Entscheidungsentwurf der französischen Aufsichtsbehörde bezüglich der «Verhaltensregeln für Dienstleistungserbringer in der klinischen Forschung» von EUCROF (Frankreich);
- eine Stellungnahme zur «Wirksamkeit von Einwilligungen im Kontext von «Consent-or-Pay»-Modellen grosser Online-Plattformen» (Niederlande zusammen mit Deutschland und Norwegen);
- eine Stellungnahme zum Begriff der Hauptniederlassung eines Verantwortlichen in der Union gemäss Art. 4 Ziff. 16 Bst. a DSGVO (Frankreich);
- eine Stellungnahme zum Einsatz von Gesichtserkennung zur Straffung der Fluggastströme (Vereinbarkeit mit Art. 5 Abs. 1 Bst. e und f, Art. 25 und Art. 32 DSGVO) (Frankreich);
- eine Stellungnahme zum Listenentwurf der lettischen Aufsichtsbehörde bezüglich Verarbeitungstätigkeiten, die von der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung ausgenommen sind (Art. 35 Abs. 5 DSGVO) (Lettland);
- fünf Stellungnahmen zu je einem Entwurf der Akkreditierungsanforderungen für eine Zertifizierungsstelle gemäss Art. 42 Abs. 5 DSGVO (Deutschland, Niederlande, Österreich);
- eine Stellungnahme zum Entwurf der Akkreditierungsanforderungen für eine Zertifizierungsstelle gemäss Art. 43 Abs. 3 DSGVO (Schweden);
- 15 Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (Accenture Group, Aptiv Group, zwei zu Avature Group, Booking.com Group, FCC Group, Genpact Group, zwei zu Infosys Group, Ivoclar Vivadent Group, MAPFRE Group, Mercans Group, Talan Group, TELEFÓNICA Group, Viega Group).

Die im Berichtsjahr vom EDSA **angenommenen Leitlinien** befassen sich mit folgenden Themen:

- Leitlinien zu Artikel 37 der Strafverfolgungsrichtlinie (EDPB Guidelines 01/2023);
- Leitlinien zum technischen Anwendungsbereich von Artikel 5(3) der Datenschutzrichtlinie für elektronische Kommunikation (EDPB Guidelines 02/2023).

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

- Leitlinien zur Verarbeitung personenbezogener Daten auf der Grundlage von Art. 6 Abs. 1 Bst. f DSGVO (EDPB Guidelines 1/2024);
- Leitlinien zu Artikel 48 DSGVO (EDPB Guidelines 2/2024).

Empfehlungen hat der EDSA im Berichtsjahr keine verabschiedet.

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 ganz unterschiedlichen Themen Einsitz, welche nachfolgend dargestellt werden. Die Mitarbeitenden der DSS haben 2024 an insgesamt 143 Sitzungen des Ausschusses und solcher Arbeitsgruppen teilgenommen.

Die spezielle Taskforce des EDSA zu Bussgeldern gemäss DSGVO *(Taskforce Fining)* befasst sich mit der konkreten Berechnung von Bussgeldern und verfolgt das Ziel, eine möglichst einheitliche europäische Praxis zu etablieren.

Im Berichtsjahr setzte die Taskforce die Überarbeitung des zentralen Bussgeldregisters des EDSA fort und vertiefte die Diskussion über die Methodik zur Berechnung von Bussgeldern bei mehreren gleichzeitigen Verstössen gegen die DSGVO (Art. 83 Abs. 3 DSGVO). Ein besonderer Fokus lag dabei auf den möglichen Konsequenzen aus den EuGH-Urteilen C-683/21 und C-807/21, die sich mit der Abgrenzung von Fahrlässigkeit und Absicht in Datenschutzverstössen befassten.

Darüber hinaus tauschten sich die Mitglieder der Taskforce über wesentliche nationale Bussgeldentscheidungen sowie relevante Gerichtsurteile aus. Ein weiterer Schwerpunkt war die Überarbeitung der Leitlinien zur Anwendung und Festsetzung von Geldbussen (WP 253), die ursprünglich von der ehemaligen Artikel-29-Datenschutzgruppe erarbeitet wurden und nun an die aktuelle Rechtsprechung und Durchsetzungspraxis angepasst werden sollen.

Die Arbeitsgruppe des EDSA, welche sich mit der möglichst einheitlichen Durchsetzung der Bestimmungen der DSGVO in den Mitgliedstaaten befasst *(Enforcement Subgroup)*, war im Berichtsjahr erneut mit der Durchführung von einem Verfahren im Rahmen des Streitbeilegungsmechanismus gemäss Art. 65 DSGVO beschäftigt. Zwei betroffene Aufsichtsbehörden hatten massgeblichen und begründeten Einspruch gegen den Beschlussentwurf der federführenden Aufsichtsbehörde eingelegt, dem sich diese jedoch nicht angeschlossen bzw. den diese abgelehnt hatte. Der in solchen Fällen erforderliche verbindliche Beschluss des EDSA zur Streitbeilegung wurde von der Arbeitsgruppe vorbereitet. Des Weiteren hat die Arbeitsgruppe erneut das Projekt der «strategischen Fälle» diskutiert sowie den Fortschritt in den einzelnen Fällen verfolgt. Die DSS beteiligte sich im Berichtsjahr weiter an der gemeinsamen Untersuchung mehrerer Aufsichtsbehörden zu Smart TVs. Daneben hat die Arbeitsgruppe die Arbeit an Leitlinien zu Art. 66 DSGVO aufgenommen und ein über alle Behörden einheitliches Reporting diskutiert und als Pilotprojekt gestartet.

Wertvoll aus Sicht der DSS war darüber hinaus auch 2024 wieder der im Rahmen der Arbeitsgruppe regelmässig geführte Austausch über grössere laufende Verfahren oder wichtige Entscheidungen der Aufsichtsbehörden in ihren jeweiligen Ländern. Speziell wurde im Berichtsjahr über Verfahren und Entscheidungen in den Bereichen Speicherung von Kreditkarteninformationen für künftige Online-Einkäufe, Datenverarbeitung in der Mobilitäts-Industrie, Videoüberwachung sowie Transparenz bei der Datenverarbeitung im Finanzsektor gesprochen.

Die Arbeit am Projekt zum Recht auf rechtliches Gehör in datenschutzrechtlichen Verfahren, woran die DSS als Co-Rapporteur beteiligt ist, wurde im Berichtsjahr angesichts des Gesetzesentwurfs der EU-Kommission für weitere harmonisierte Verfahrensregelungen zur Durchsetzung der DSGVO pausiert. Darüber hinaus wurden die Arbeiten im Rahmen der *Taskforce 101* und der *Cookie Banner Taskforce* abgeschlossen. Erstere strebte die möglichst einheitliche Beurteilung der 101 Beschwerden der Organisation *None of Your Business (noyb)* des Datenschutz-Aktivisten Max Schrems zum Einsatz von Google Analytics und Facebook Pixel auf Webseiten durch die betroffenen Aufsichtsbehörden an. Die *Cookie Banner Taskforce* behandelte diverse Fragen rund um die rechtlich zulässige oder unzulässige Gestaltung von Cookie-Bannern. Nach erfolgreichem Abschluss ihrer Arbeit wurden beide Taskforces im Berichtsjahr aufgelöst. Daneben wurde im Vorjahr noch eine weitere Taskforce zu datenschutzrechtlichen Fragen rund um die Anwendung von ChatGPT *(ChatGPT Taskforce)* gegründet, welche die Zusammenarbeit und den Informationsaustausch zwischen den Aufsichtsbehörden bei Untersuchungen und Verfahren in Zusammenhang mit ChatGPT/OpenAI bezweckt. Sie hat 2024 einen Bericht über ihre Arbeit publiziert.

Die Arbeitsgruppe zur möglichst einheitlichen Durchsetzung der Bestimmungen der DSGVO in den Mitgliedstaaten *(Enforcement Subgroup)* hat schliesslich auch das *Coordinated Enforcement Framework* ins Leben gerufen, im Rahmen dessen jedes Jahr von europäischen Aufsichtsbehörden gemeinsam ein bestimmtes datenschutzrechtliches Thema europaweit untersucht wird (Coordinated Action). 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 welche Mittel sie einsetzen möchte.

Im Berichtsjahr wurde eine solche *Coordinated Action* zum Auskunftsrecht gemäss Art. 15 DSGVO durchgeführt. Die DSS hat sich daran beteiligt und einen umfangreichen Fragebogen an fünf grosse Organisationen verschiedener Sektoren und Branchen

in Liechtenstein verschickt. Ziel war die Erhebung von Informationen zur konkreten Umsetzung dieses Betroffenenrechts in den ausgewählten Organisationen. Die Antworten wurden von der DSS in einem nationalen Bericht zusammengefasst und die wichtigsten Erkenntnisse daraus sowie konkrete Handlungsempfehlungen den betrieblichen Datenschutzbeauftragten in Liechtenstein am jährlichen Vernetzungstreffen präsentiert. Der über alle teilnehmenden Länder aggregierte Abschlussbericht des EDSA wird auf europäischer Ebene anfangs 2025 veröffentlicht werden. Durch die im Rahmen solcher koordinierten Aktionen gewonnenen Erkenntnisse kann die DSS die Organisationen in Liechtenstein noch besser unterstützen, indem sie zielgerichtete Weiterbildungen, Informationen und Beratung anbietet.

Für 2025 wurde bereits wieder eine neue *Coordinated Action* lanciert, welche sich mit der Umsetzung des Rechts auf Löschung gemäss Art. 17 DSGVO befasst. Auch daran wird sich die DSS erneut aktiv beteiligen.

Von der Arbeitsgruppe, welche sich mit der Zusammenarbeit der Aufsichtsbehörden befasst *(Cooperation Subgroup)*, wurde im Berichtsjahr insbesondere das Gesetzgebungsvorhaben der EU-Kommission für weitere harmonisierte Verfahrensregelungen zur Durchsetzung der DSGVO eng begleitet und erneut eine Stellungnahme dazu abgegeben. Zudem hat die Arbeitsgruppe die Überarbeitung der Leitlinien zu Art. 61 DSGVO weitergeführt sowie zu Art. 62 DSGVO und Art. 64(2) DSGVO neu aufgenommen. Ebenso konnte ein gemeinsames europäisches Register der Vertreter gemäss Art. 27 DSGVO von Organisationen aus Drittstaaten eingeführt werden. Ein weiterer Diskussionspunkt war die Anwendung bzw. Nicht-Anwendung des One-Stop-Shop Mechanismus (formelle Zusammenarbeit der Datenschutzbehörden in grenzüberschreitenden Fällen) in Situationen, in denen nationales Recht involviert ist (Art. 55 DSGVO).

Die thematische Arbeitsgruppe zu Finanzangelegenheiten des EDSA *(Financial Matters Subgroup)* hat im Berichtsjahr das voranschreitende Projekt der Europäischen Zentralbank zur Einführung eines Digitalen Euros weiter eng verfolgt. Zudem wurde mit der Europäischen Bankenaufsichtsbehörde ein regelmässiger Austausch zu relevanten datenschutzrechtlichen Themen und zur künftigen Zusammenarbeit im Rahmen der europäischen Regulierung zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung (AML/CFT) gestartet. Daneben wurde von der Arbeitsgruppe aber auch die Arbeit an Leitlinien des EDSA zum Datenschutz bei der Bekämpfung von Geldwäscherei und Terrorismusfinanzierung (AML/CFT) weitergeführt, vorerst insbesondere zum Thema der Nutzung so genannter Watch Lists durch regulierte Finanzintermediäre. Darüber hinaus hat die Arbeitsgruppe diverse Diskussionen geführt sowie kleinere Beiträge und Stellungnahmen erarbeitet zu Themen wie Zahlungsbetrug, zwingende Nutzerkontoeröffnung in Online-Shops, Open Finance oder zum Regulierungspaket der EU-Kommission für den Zugang zu Finanzdaten und Zahlungsverkehr. Viele dieser Arbeiten werden auch 2025 fortgeführt. Schliesslich fand mit der EDSA-Arbeitsgruppe zu internationalen Datentransfers angesichts eines entsprechenden Ansuchens der EU-Ratspräsidentschaft an den EDSA ein Austausch zu Datenübermittlungen im Finanzbereich, insbesondere bezüglich des Automatischen Informationsaustausches zu Steuerzwecken, statt.

Im Berichtsjahr wurde ausserdem entschieden, die *Taskforce Competition and Consumer Law* zur Untersuchung der Zusammenhänge zwischen Datenschutz und Wettbewerbsrecht künftig in eine längerfristige Arbeitsgruppe des EDSA umzuwandeln.

Die Arbeitsgruppe zu Datenübermittlungen in Drittstaaten *(International Transfer Subgroup)* hat im Berichtsjahr an 14 Sitzungen ihre Arbeiten zu diversen Themen aufgenommen oder fortgesetzt. Die noch nicht abgeschlossene Überarbeitung der Empfehlungen für verbindliche interne Datenschutzvorschriften für Auftragsdatenverarbeiter («Processor BCR») orientierte sich an den bereits verabschiedeten Empfehlungen für Verantwortliche wie auch dem entsprechenden, bereits unter der ehemaligen Artikel-29-Datenschutzgruppe ausgearbeiteten Dokument. Auch eine Diskussion bezüglich des internen BCR-Verfahrens, also wie die Kooperation zwischen den einzelnen Aufsichtsbehörden dabei aussieht und welche Schritte und Prozesse durchlaufen und eingehalten werden müssen, wurde im Berichtsjahr fortgeführt. Ziel ist es insbesondere, den Prozess zu beschleunigen, ohne an Qualität einzubüssen. Auch hier konnte jedoch noch kein finales Dokument ausgearbeitet werden. Weiters wurden im Berichtsjahr Leitlinien zu Art. 48 DSGVO erarbeitet und veröffentlicht. Sie bieten praktische Empfehlungen für Verantwortliche und Auftragsverarbeiter im EU/EWR-Raum bei Anfragen von Gerichten und Behörden aus Drittstaaten zur Datenweitergabe. Die Kernaussage von Art. 48 DSGVO ist, dass Urteile oder Entscheidungen aus Drittstaaten nicht automatisch in der EU bzw. im EWR anerkannt oder vollstreckt werden können. Stattdessen erfolgt eine Anerkennung nur auf Grundlage internationaler Abkommen, um die rechtliche Souveränität der EU bzw. der EU/EWR-Mitgliedstaaten zu wahren.

Zu Beginn des Berichtsjahres veröffentlichte die EU-Kommission ihren Bericht zur ersten Überprü-

fung der Angemessenheitsentscheidungen, die bereits im Rahmen der früheren «Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr» von ihr erlassen wurden. Im Zuge dieser Überprüfung wurden sowohl der Angemessenheitsbeschluss für die Schweiz als auch diejenigen für zehn weitere Staaten gemäss Art. 45 DSGVO bestätigt. Um die Konformität mit den europäischen Datenschutzstandards zu gewährleisten, verlangte die EU-Kommission jedoch noch gezielte Anpassungen und Ergänzungen der nationalen Datenschutzregelungen in den betroffenen Staaten. Diese Massnahmen führten letztlich zu einer positiven Neubewertung und Bestätigung der Angemessenheitsentscheidungen.

Die zuständige Arbeitsgruppe verfolgte diese Entwicklungen kontinuierlich und mit grosser Aufmerksamkeit, um sicherzustellen, dass die erforderlichen Anpassungen im Einklang mit den europäischen Datenschutzstandards vorgenommen wurden. Gerade für Liechtenstein ist die Bestätigung des Angemessenheitsbeschlusses für die Schweiz von besonderer Bedeutung, da zwischen beiden Ländern enge wirtschaftliche und rechtliche Verflechtungen bestehen, die auch den Datentransfer betreffen.

Ein wichtiges Thema für die Arbeitsgruppe war im Berichtsjahr auch die geplante Anpassung der nationalen Datenschutzgesetzgebung im Vereinigten Königreich Grossbritannien und Nordirland (Vereinigtes Königreich). Da im Vereinigten Königreich vor dem Brexit die DSGVO anwendbar war, konnte nach dem Austritt einfach ein Angemessenheitsbeschluss gemäss Art. 45 DSGVO für den Datentransfer zwischen der EU und dem Vereinigten Königreich von der EU-Kommission erlassen werden. Mögliche Gesetzesänderungen im Vereinigten Königreich könnten nun aber Auswirkungen auf diesen Beschluss haben, der im Jahr 2025 ausläuft und von der EU-Kommission neu überprüft wird. Aufgrund der engen wirtschaftlichen Verbindungen zwischen der EU und dem Vereinigten Königreich wird dieser Prozess besonders aufmerksam verfolgt.

Darüber hinaus befasste sich die Arbeitsgruppe mit dem EU-U.S. Data Privacy Framework (EU-U.S. DPF), das als Angemessenheitsbeschluss für teilnehmende Unternehmen in den USA dient. Im Berichtsjahr fand die erste Überprüfung dieses Abkommens statt. Ende des Jahres veröffentlichte der EDSA einen Bericht, der die Bemühungen der U.S.-Behörden und der EU-Kommission bei der Umsetzung des EU-U.S. DPF hervorhob. Besonders gewürdigt wurden dabei die Einführung des Zertifizierungsprozesses sowie die Implementierung von Beschwerdemechanismen für Personen im EU/EWR-Raum, die eine bessere Durchsetzung des Datenschutzes in den transatlantischen Datenströmen ermöglichen sollen.

Die CEH-Arbeitsgruppe *(CEH Expert Subgroup)*, eine Kurzbezeichnung für Compliance, E-Government und Health, befasst sich mit Themen wie Zertifizierung und Akkreditierung sowie E-Government und dem Gesundheitsbereich. 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 gemäss Art. 64 DSGVO abgab. Konkret waren dies im Berichtsjahr die Verhaltensregeln für Dienstleistungsanbieter in Klinischer Forschung von EUCROF, die Zertifizierungskriterien von EuroPriSe Cert GmbH, die Zertifizierungskriterien von DSGVO-zt GmbH, ein Katalog von Kriterien für die Zertifizierung von IT-unterstützter Verarbeitung personenbezogener Daten von datenschutz cert GmbH sowie die Zertifizierungskriterien von Brand Compliance. Die CEH-Arbeitsgruppe bemüht sich auch um die Erarbeitung gemeinsamer Standards und die Förderung fachspezifischen Know-hows bei den Mitarbeitenden in den Aufsichtsbehörden, die sich mit Akkreditierung und Zertifizierung befassen. Dazu wurden im Berichtsjahr Workshops angeboten.

Im Bereich E-Government verfolgte die CEH-Arbeitsgruppe 2024 insbesondere die massgebenden Entwicklungen bei den europäischen Digitalisierungsrechtsakten. Im Gesundheitsbereich widmete sie sich dem Entwurf von Leitlinien zur Verarbeitung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung. Hierzu wurden verschiedene offene Detailfragen analysiert und konnten einer gemeinsamen Lösung zugeführt werden. Aufgrund der Komplexität der Materie konnten die Leitlinien im Berichtsjahr aber noch nicht final abgeschlossen werden.

Künstliche Intelligenz war im Berichtsjahr eines der Schwerpunktthemen der Arbeitsgruppe zu technologischen Themen *(Technology Expert Subgroup)*. Im Juli verabschiedete der EDSA die Stellungnahme zur Rolle der Datenschutzbehörden im Rahmen der Verordnung der Europäischen Union über künstliche Intelligenz (KI-Verordnung), welche von der Arbeitsgruppe vorbereitet wurde. Zusammenfassend stellt die Stellungnahme klar, dass die Datenschutzbehörden neben der DSGVO auch bei der Überwachung der Einhaltung der KI-Verordnung eine wichtige Rolle spielen werden. Im Dezember veröffentliche der EDSA

auf Antrag der irischen Datenschutzbehörde zudem eine Stellungnahme zu bestimmten Datenschutzaspekten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Kontext von KI-Modellen, an deren Ausarbeitung die Arbeitsgruppe massgeblich beteiligt war. Zusammengefasst behandelt diese Stellungnahme die Bedingungen für die Anonymität von KI-Modellen, die Möglichkeit der Verwendung des berechtigten Interesses als Rechtsgrundlage für ihre Entwicklung oder Nutzung sowie die Konsequenzen der Verwendung unrechtmässig verarbeiteter personenbezogener Daten bei der Entwicklung von KI-Modellen. Im Rahmen des Verfahrens zur Erarbeitung dieser Stellungnahme wurde auch eine öffentliche Konsultation durchgeführt. Diese ermöglichte es interessierten Akteuren aus Wirtschaft, Forschung und Zivilgesellschaft, ihre Ansichten vorab mit dem EDSA zu teilen und zu diskutieren.

Die Leitlinie zur Pseudonymisierung konnte ebenfalls im Berichtsjahr von der Arbeitsgruppe fertiggestellt werden. Ihre Verabschiedung durch den EDSA wird für Anfang 2025 erwartet. Anders sieht es bei der ebenfalls geplanten Leitlinie zur Anonymisierung aus. Insbesondere aufgrund der sehr engen Verzahnung von Anonymisierung und künstlicher Intelligenz und der damit verbundenen Komplexität der Anonymisierung in KI-Modellen wird die Erarbeitung dieser Leitlinie noch einige Zeit in Anspruch nehmen. Daneben hat die Arbeitsgruppe im Berichtsjahr auch die Arbeit an einer Leitlinie zu generativer KI aufgenommen. Und sie wurde mehrfach von anderen Arbeitsgruppen zu technischen Themen konsultiert.

Die Arbeitsgruppe zu Sozialen Medien *(Social Media Subgroup)* stellte 2024 die Ausarbeitung von Leitlinien zur Nutzung sozialer Medien durch öffentliche Stellen in den Mittelpunkt ihrer Tätigkeiten, mit dem Ziel, diese noch im Berichtsjahr zu verabschieden. Da im Ausschuss allerdings der für die Verabschiedung erforderliche Konsens nicht gefunden werden konnte, wird die Arbeitsgruppe das Dokument 2025 nochmals überarbeiten. Parallel wurde an den Leitlinien über das Zusammenspiel zwischen dem Gesetz über digitale Dienste (Digital Services Act; DSA) und der DSGVO weitergearbeitet.

Im Berichtsjahr nahm die DSS ihre Teilnahme an der BTLE-Arbeitsgruppe *(Border Travel and Law Enforcement Expert Subgroup)* wieder aktiv auf. Diese Arbeitsgruppe koordiniert die zentralen datenschutzrechtlichen Entwicklungen in den Bereichen Polizei, Grenzverkehr und Strafjustiz. Ein wesentlicher Schwerpunkt ihrer Arbeit war 2024 die Erarbeitung und Fertigstellung von Leitlinien zu den datenschutzrechtlichen Garantien bei der Übermittlung personenbezogener Daten in Drittstaaten gemäss Art. 37 der Strafverfolgungsrichtlinie sowie die Mitarbeit an den Leitlinien zu Art. 48 DSGVO, die sich derzeit in der Phase der öffentlichen Konsultation befinden.

Daneben beteiligte sich die Arbeitsgruppe an der Überprüfung zahlreicher Angemessenheitsentscheidungen für Drittstaaten gemäss Art. 45 DSGVO, die mindestens alle vier Jahre von der EU-Kommission überprüft werden müssen. Die BTLE-Arbeitsgruppe unterstützte diese Prüfungen durch Analysen zu Datenschutzfragen im Strafverfolgungskontext und arbeitete dabei mit der Arbeitsgruppe zu Datenübermittlungen in Drittstaaten zusammen. Zudem wurde im Berichtsjahr auch die Arbeitsgruppe zu technologischen Themen unterstützt, welche bei der Erarbeitung von Leitlinien zum Zusammenspiel zwischen KI-Verordnung und EU-Datenschutzrecht mit spezifischen Fragen an die BTLE-Arbeitsgruppe herantrat. Diese betrafen vor allem die Vereinbarkeit von Hochrisiko-KI-Systemen mit geltenden Datenschutzbestimmungen.

Die BTLE-Arbeitsgruppe unterstützte darüber hinaus die Umsetzung des Beschwerdeverfahrens im Rahmen des EU-U.S. Data Privacy Framework (DPF), indem sie die Struktur des Verfahrens festlegte, ein standardisiertes Beschwerdeformular entwarf und die Verfahrensregeln dafür erstellte. Das auf diese Weise standardisierte Verfahren soll betroffenen Personen die Einreichung von Beschwerden im Rahmen des EU-U.S. DPF erleichtern. Zudem trugen die Mitglieder zur Übersetzung des Formulars in alle offiziellen Amtssprachen des EU/EWR-Raumes bei.

Schliesslich erarbeitete die Arbeitsgruppe 2024 auch eine Stellungnahme zu den Empfehlungen der High-Level Group on Access to Data for Effective Law Enforcement. Die Stellungnahme konzentrierte sich auf Themen wie einheitliche Regeln zur Datenspeicherung, Datensicherheit und Verschlüsselung sowie den Schutz der Grundrechte im Kontext des Datenzugriffs durch Strafverfolgungsbehörden. Dabei wurde auch diskutiert, ob die Empfehlungen der High-Level Group ausreichende objektive Gründe enthalten, um den angestrebten Zugriff zu rechtfertigen.

Ab dem Berichtsjahr hat die DSS auch wieder regelmässig an den Sitzungen der Arbeitsgruppe zu Schlüsselthemen der DSGVO *(Key Provisions Expert Subgroup)* teilgenommen. Die Arbeitsgruppe befasst sich mit den zentralen Bestimmungen der DSGVO und entwickelt dazu grundlegende Empfehlungen zur Auslegung und praktischen Anwendung der Datenschutzvorschriften. Diesen Arbeiten kommt eine besondere Bedeutung im Hinblick auf die einheitliche Rechtsanwendung der Vorschriften zu.

Ein erster bedeutender Meilenstein der Tätigkeit dieser Arbeitsgruppe im Berichtsjahr war die Veröffentlichung von Leitlinien zur Verarbeitung personenbezogener Daten auf Grundlage von Art. 6 Abs. 1 Bst. f DSGVO (berechtigtes Interesse). Die öffentliche Konsultationsphase ist mittlerweile abgeschlossen und die Arbeitsgruppe befindet sich nun in der finalen Überarbeitungsphase der Leitlinien unter Berücksichtigung der erhaltenen Rückmeldungen. Diese Leitlinien sollen Verantwortlichen einen dreistufigen Prüfungsansatz zur rechtssicheren Anwendung dieser nicht immer einfachen Rechtsgrundlage bieten. Parallel dazu arbeitete die Arbeitsgruppe im Berichtsjahr auch an Leitlinien zu Daten von Kindern, zu Kriterien für Altersverifikation sowie der Aktualisierung der Leitlinien für Datenschutzbeauftragte (DPO).

Ein weiterer und nach wie vor andauernder Arbeitsschwerpunkt war die Ausarbeitung der Leitlinien zu «Consent-or-Pay»-Modellen. Auch diese Leitlinien befinden sich noch in der Entwicklungsphase. Sie sollen die Voraussetzungen für eine gültige Einwilligung unter der DSGVO, insbesondere im Kontext grosser Online-Plattformen, präziser definieren. Nach einer ersten Stellungnahme des EDSA gemäss Art. 64 Abs. 2 DSGVO zu diesem Thema wurde die Arbeitsgruppe beauftragt, ergänzende Leitlinien zu entwickeln. Um dabei einen partizipativen Ansatz zu gewährleisten, organisierte der EDSA am 18. November einen Anlass für interessierte Akteure, an dem diese die Gelegenheit bekamen, ihre Perspektiven auf das Thema einzubringen.

Zusätzlich fanden im Berichtsjahr mehrere Konsultationen durch die Arbeitsgruppe zu technologischen Themen statt, im Rahmen derer spezifische Fragen zu Anonymisierung und Pseudonymisierung erörtert wurden. Daneben wurden auch Aspekte des Einsatzes von generativer KI und deren Auswirkungen auf den Datenschutz diskutiert. Diese vielfältigen Tätigkeiten zeigen die bedeutende Rolle dieser Arbeitsgruppe bei der Sicherstellung einer konsistenten und rechtlich fundierten Anwendung der DSGVO.

Die spezielle Taskforce zum internationalen Engagement der Mitglieder *(Taskforce on International Engagement)* wurde bereits im Vorjahr vom EDSA ins Leben gerufen und seit dem Berichtsjahr nimmt auch die DSS an ihren Sitzungen teil. Ihr Ziel ist es, den Austausch zwischen den EDSA-Mitgliedern zu fördern hinsichtlich deren Teilnahme in multilateralen Foren zum Datenschutz und Schutz der Privatsphäre wie etwa dem Europarat, 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. Es soll die Teilnahme von EDSA-Mitgliedern besser koordiniert, der Austausch von Informationen über globale Datenschutzentwicklungen vereinfacht sowie die Schaffung einer einheitlichen europäischen Position in internationalen Debatten gefördert werden.

Im Berichtsjahr widmete sich die Taskforce datenschutzrechtlichen Themen, die in internationalen Foren wie der GPA diskutiert wurden. Dazu gehörten etwa die Auswirkungen von Künstlicher Intelligenz, Altersverifikationsmechanismen und internationale Regelungen zur Datenübertragung. Bezüglich des G7 DPAR lag der Fokus vor allem auf den Herausforderungen des Datenschutzes im digitalen Zeitalter und der Rolle von Datenschutz-Aufsichtsbehörden bei der Regulierung von Künstlicher Intelligenz.

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 Erfahrungsaustausch unter den Datenschutzbeauftragten sowie die Erleichterung ihrer Arbeit durch Schaffung einheitlicher Standards. Über dieses primäre Ziel hinaus widmet sich das DPO-Network auch den ihm durch den EDSA zugewiesenen spezifischen Themen. Entsprechend der Zielsetzung des DPO-Netzwerkes befasste sich das DPO-Netzwerk auch dieses Jahr mit relevanten Fragestellungen und Themen in diesem Bereich. Im Berichtsjahr fanden jedoch aufgrund anderer prioritär zu behandelnden Agenden auf europäischer Ebene keine Sitzungen statt. Die Möglichkeit des Austauschs über das eingerichtete Forum war allerdings stets möglich und die Zielsetzung des DPO-Netzwerks auch damit erreicht.

7.1.3 BCR-Workshop

Die europäischen Datenschutzaufsichtsbehörden organisieren regelmässig Workshops und Fachtreffen zum Thema der verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules; BCR), um den internationalen Austausch und die Harmonisierung des Verfahrens sowie der Genehmigungsanforderungen in diesem Bereich zu fördern. Seit dem Inkrafttreten der DSGVO fanden bereits drei dieser Workshops statt: 2019 in Norwegen, 2022 in Kroatien und im Berichtsjahr in Litauen.

Diese Treffen verfolgen zwei zentrale Ziele: Zum einen sollen neue Mitglieder von Datenschutz-Aufsichtsbehörden die Möglichkeit erhalten, sich mit der Materie der BCR sowie dem Genehmigungsverfahren vertraut zu machen. Zum anderen können sich erfahrene Experten zu aktuellen Fragestellungen austauschen, um ein einheitliches Verständnis

der BCR-Voraussetzungen zu fördern und gemeinsame Herausforderungen zu diskutieren.

Ein besonders intensiv behandeltes Thema war der Umgang mit BCR, die gleichzeitig als umfassendes globales Datenschutzreglement (Global Privacy Policy) eines Unternehmens dienen und damit weit über den ursprünglichen Rahmen der BCR hinausgehen, welche nur den internationalen Transfer von Daten in Drittstaaten regeln. Dies wirft unter anderem Fragen zur Transparenz und zur Bestimmung des anwendbaren Rechts auf.

Die Erfolgsgeschichte der BCR, die ursprünglich im EU/EWR-Raum begann, hat mittlerweile international Einfluss genommen. Immer mehr Drittländer haben ähnliche Genehmigungsverfahren für BCR eingeführt. Dies ist grundsätzlich eine begrüssenswerte Entwicklung, bringt jedoch neue Herausforderungen für die Umsetzung und Genehmigung innerhalb des EU/EWR-Raum mit sich. Eine zentrale Fragestellung ist dabei, wie Klage- und Beschwerdemöglichkeiten für betroffene Personen in diesen neuen internationalen Regelwerken ausgestaltet werden sollen.

Im Rahmen des BCR-Workshops in Litauen hielt die DSS gemeinsam mit Kollegen aus den Niederlanden einen Vortrag und leitete eine Diskussion zu diesen komplexen Fragen. Der Fokus lag insbesondere auf den rechtlichen Implikationen neuer BCR-Ansätze, dem Anpassungsbedarf innerhalb des EU/EWR-Raums sowie auf der Frage, wie sich internationale Entwicklungen mit den bestehenden europäischen Datenschutzstandards vereinbaren lassen.

2026 wird der BCR-Workshop voraussichtlich in Liechtenstein stattfinden.

7.1.4 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 162 Anfragen von anderen europäischen Datenschutzaufsichtsbehörden, was im Vergleich zu den im Vorjahr erhaltenen 195 Anfragen einen leichten Rückgang 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: Marktforschung, Auskunftsrecht, «once only»-Prinzip, Zugang für politische Parteien zu Wählerlisten für Kampagnen, Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen von Versicherungsdienstleistungen, Recht auf Löschung der personenbezogenen Daten bei christlichen Vereinigungen, Einbezug von Behörden in Gesetzgebungsprozesse, Speicherung von Verdachtsmeldungen, Löschfristen, Videoüberwachung in Privathaushalten mit Angestellten, Kamerasysteme für Fahrzeugflotten, Kinderfotos auf Instagram Account einer Kindertagesstätte, Authentifizierung bei E-Banking, Zutrittskontrolle bzw. Anwesenheitsliste beim Arbeitsplatz.

Insgesamt lässt sich feststellen, dass die Amtshilfeersuchen – ähnlich wie die allgemeinen Anfragen an die DSS – zunehmend komplexer werden und sich verstärkt auf datenschutzrechtliche Fragestellungen im Zusammenhang mit neuen Technologien beziehen.

Zudem beobachtet die DSS vermehrt, dass sich einige der gestellten Anfragen auf Systeme und Technologien beziehen, die in Liechtenstein (noch) nicht zum Einsatz kommen. Dies stellt eine besondere Herausforderung dar, da es zunehmend schwieriger wird, alle diese Fragen fundiert und praxisnah zu beantworten. Infolgedessen muss die DSS priorisieren, welche Anfragen sie vertieft bearbeitet 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 bereits im Jahr 2022, eine länderübergreifende strategische Untersuchung zum Thema SmartTV zu starten. Da solche Geräte auch in Liechtenstein weit verbreitet im Einsatz sind, sagte die DSS ihre aktive Teilnahme zu. Die länderübergreifende strategische Untersuchung zum Thema SmartTV konnte allerdings im Berichtsjahr aufgrund mangelnder Ressourcen bei den teilnehmenden Behörden sowie einer Prioritätsverschiebung noch nicht abgeschlossen werden und wird daher 2025 fortgesetzt werden.

7.3 Europarat

Die DSS hat im Berichtsjahr an der 46. und 47. 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. Ausserdem hat er ein zusätzliches Set von Standardvertragsklauseln für grenzüberschreitende Datentransfers erlassen. Im Übrigen bestand die Hauptarbeit des Beratenden Ausschusses an der Erarbeitung von Berichten, Positionspapieren u.ä. etwa zur Datenverarbeitung im Rahmen von Abstimmungen und Wahlen oder zu datenschutzrechtlichen Fragen bei generativer künstlicher Intelligenz (insbesondere bei Large Language Models). Die Ergebnisse dieser Arbeiten können zu künftigen Handlungsempfehlungen, Leitlinien, Resolutionen oder Erklärungen auch übergeordneter Organe des Europarates führen.

Die Konvention 108 wurde kürzlich mittels eines Änderungsprotokolls modernisiert und insbesondere an die heutigen informations- und kommunikationstechnologischen Möglichkeiten der Datenverarbeitung angepasst. Einschliesslich Liechtenstein haben bereits 31 Staaten das Änderungsprotokoll ratifiziert. Damit fehlen nur noch 7 Ratifizierungen bis zum Inkrafttreten des Änderungsprotokolls bzw. der modernisierten Konvention 108+, was für 2025 erwartet wird. Der Beratende Ausschuss hat sich entsprechend im Berichtsjahr auch mit dem angestrebten Inkrafttreten des Änderungsprotokolls sowie der Auslegung von Art. 11 der modernisierten Konvention 108+ befasst, welcher verschiedene Ausnahmen regelt.

«Auch in Zukunft wird die DSS mit Augenmass, aber entschlossen dafür sorgen, dass Datenschutz nicht nur eine Verpflichtung, sondern auch ein gelebtes Prinzip bleibt.»

8. Schlussbemerkung und Ausblick

Ist also Datenschutz tatsächlich eine Form der «Grundversorgung» für unsere digitale Gesellschaft? Die DSS ist davon überzeugt und gewillt, ihre Arbeit auch künftig in diesem Sinne weiterzuführen.

Die Bedeutung einer funktionierenden Grundversorgung im Datenschutz wird im Jahr 2025 weiter zunehmen. Denn während sich die digitale Welt rasant weiterentwickelt, nimmt auch die Regulierungsdichte stetig zu. Mit der KI-Verordnung, dem Data Act, dem Data Governance Act, dem Digital Markets Act oder dem Digital Services Act stehen Unternehmen, öffentliche Stellen und Aufsichtsbehörden vor neuen, komplexen Anforderungen. Diese Gesetze bringen wichtige Weichenstellungen für den Schutz personenbezogener Daten in der digitalen Wirtschaft, aber auch erhebliche Herausforderungen in der praktischen Umsetzung. Gerade in Zeiten dieser tiefgreifenden regulatorischen Veränderungen muss der Datenschutz nicht nur rechtskonform, sondern auch pragmatisch und alltagstauglich gestaltet werden.

Die DSS wird sich daher auch 2025 der Aufgabe widmen, neue Datenschutzfragen mit praktikablen Lösungen zu beantworten. Denn Datenschutz-Grundversorgung bedeutet nicht nur, sich um grosse strategische Themen zu kümmern, sondern auch im konkreten Alltag für Klarheit zu sorgen – sei es für Unternehmen, die sich an die neuen Vorgaben anpassen müssen, für Bürgerinnen und Bürger, die ihre Rechte verstehen und durchsetzen möchten, oder für öffentliche Stellen, die datenschutzkonforme Prozesse etablieren müssen. Dabei ist es essenziell, nicht nur auf einzelne Vorgaben zu blicken, sondern das grosse Ganze im Auge zu behalten: Datenschutz darf nicht zu einer Hürde für Innovation und digitale Teilhabe werden, sondern muss als integraler und selbstverständlicher Bestandteil einer vertrauenswürdigen digitalen Gesellschaft gestaltet werden.

Gerade die Regulierung Künstlicher Intelligenz wird eine zentrale Rolle spielen. Systeme, die automatisierte Entscheidungen treffen, personenbezogene Daten auswerten oder Verhaltensanalysen durchführen, müssen so reguliert werden, dass sie Innovation ermöglichen, ohne Grundrechte zu gefährden. Hier gilt es, klare und zugleich umsetzbare Antworten zu finden – denn zu viel Bürokratie bremst den Fortschritt, während zu wenig Schutz das Vertrauen in digitale Technologien untergräbt. Ein ausgewogener Ansatz ist gefragt, der technologische Entwicklungen nicht ausbremst, aber auch den Schutz der Privatsphäre nicht vernachlässigt.

Selbstverständlich wird auch die aufsichtsrechtliche Tätigkeit der DSS im Jahr 2025 eine zentrale Rolle spielen. Die Durchsetzung des Datenschutzrechts bleibt essenziell, um sicherzustellen, dass die bestehenden und neuen Anforderungen nicht nur auf dem Papier stehen, sondern auch in der Praxis wirksam umgesetzt werden. Die Verfahrensführung ist dabei ein wichtiger Bestandteil unserer Arbeit – sei es bei der Bearbeitung von Beschwerden, der Durchführung von Untersuchungen oder der Klärung rechtlicher Fragen. Bussgelder können, wie bereits in diesem Jahr, als wirksames Mittel zum Einsatz kommen, um Verstösse zu sanktionieren und eine konsequente Anwendung des Datenschutzrechts sicherzustellen. Auch in Zukunft wird die DSS mit Augenmass, aber entschlossen dafür sorgen, dass Datenschutz nicht nur eine Verpflichtung, sondern auch ein gelebtes Prinzip bleibt.

Mit Blick auf die neuen Rechtsakte der EU, aber auch nationaler Digitalisierungsvorhaben wird sich die DSS verstärkt mit den Schnittstellen zwischen Datenschutz und anderen digitalen Regulierungen beschäftigen. Es wird entscheidend sein, dass Datenschutz nicht isoliert betrachtet wird, sondern sich harmonisch in das Gesamtgefüge der digitalen Gesetzgebung einfügt. Nutzerrechte, Transparenzpflichten und Marktregulierungen müssen so zusammenspielen, dass Datenschutz nicht zum Stolperstein wird, sondern zu einem integrativen Bestandteil eines fairen und sicheren digitalen Ökosystems.

Damit all diese Veränderungen nicht nur abstrakte Regulierung bleiben, sondern in der Praxis auch funktionieren, wird die DSS weiterhin für pragmatische, verständliche und umsetzbare Lösungen eintreten. Datenschutz-Grundversorgung bedeutet, zugänglich zu sein, Fragen verständlich zu beantworten und mit Augenmass vorzugehen – gerade dann, wenn der rechtliche Rahmen immer komplexer wird. Die DSS wird diesen Weg weiter entschlossen gehen und sich als verlässlicher Partner für alle Datenschutzfragen positionieren.

Datenschutzstelle Fürstentum Liechtenstein
Kirchstrasse 8
Postfach 684
FL-9490 Vaduz

Telefon +423 236 60 90
info.dss@llv.li
www.datenschutzstelle.li