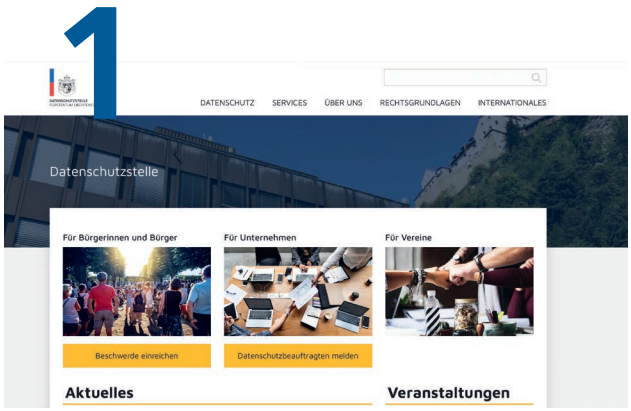
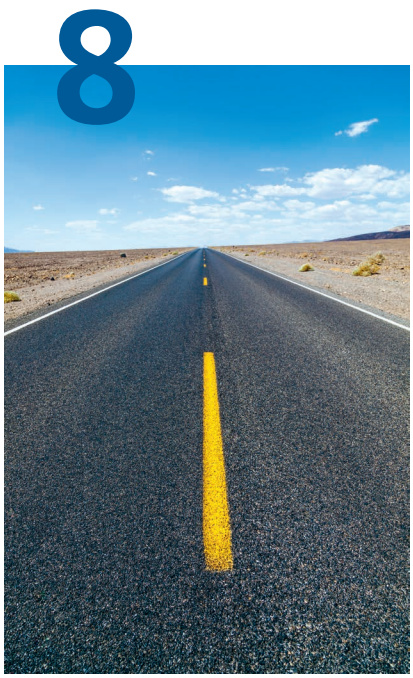
DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht Datenschutzstelle
Fürstentum Liechtenstein

Tätigkeitsbericht 2023

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 2023 wird zweifellos wegen des neuen Angemessenheitsbeschlusses (EU-U.S. Data Privacy Framework) für die USA in Erinnerung bleiben. Schliesslich hatte das Thema des fehlenden Beschlusses nach dem Urteil des Europäischen Gerichtshofes im Sommer 2020 drei Jahre lang für mehr Aufregung gesorgt als jedes andere Thema. Für die Datenschutzstelle (DSS) hingegen war es lediglich eine Frage, die nun bis auf Weiteres wohl gelöst war, aber schnell von zahlreichen neuen Fragestellungen überholt wurde.

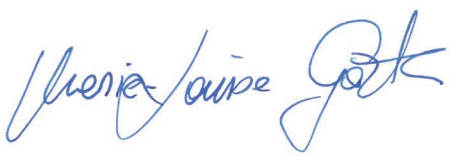
Die rasante Abfolge von Themen, die sich im Laufe des Berichtsjahres entwickelten, spiegelte sich deutlich in sämtlichen Bereichen der Tätigkeit der DSS wider, sowohl in quantitativer als auch in qualitativer Hinsicht. Über die letzten drei Jahre hinweg zeigte sich zudem eine kontinuierliche Zunahme der Komplexität der Anfragen, ein Trend, der sich auch im Berichtsjahr fortsetzte. Die rasante technologische Entwicklung brachte eine Vielzahl neuer und anspruchsvoller Fragen mit sich, insbesondere im Hinblick auf die Fähigkeit technischer Systeme, Datenschutzanforderungen zu erfüllen. Die Thematik der Künstlichen Intelligenz (KI), vor allem im Kontext von ChatGPT, führte zu zahlreichen Anfragen seitens der Verantwortlichen. Die Vielzahl von Anwendungsmöglichkeiten für KI in sämtlichen Wirtschafts- und Verwaltungsbereichen bringt nicht nur Chancen, sondern auch erhebliche Herausforderungen mit sich. Die potenziellen Risiken reichen vom Missbrauch und der Diskriminierung bis hin zur Falschinformation. Dies forderte die DSS heraus, vertiefte Kenntnisse im rechtlichen und technischen Bereich bereitzustellen, um eine umfassende Unterstützung bieten zu können.

Neben der verstärkten Inanspruchnahme der Beratungsleistungen der DSS zeichnete sich im Berichtsjahr ein weiterer bedeutsamer Trend ab: eine zunehmende Skepsis der Bevölkerung gegenüber Datenverarbeitungen durch private und öffentliche Stellen. Diese Skepsis manifestierte sich nicht nur in einer steigenden Anzahl von Beschwerden, sondern auch in äusserst kritischen Anfragen an die DSS. Darüber hinaus zeigte sich eine wachsende Bereitschaft der Verfahrensparteien, Beschwerde gegen die Entscheidungen der DSS bei der Beschwerdekommission für Verwaltungsangelegenheiten einzulegen und gegebenenfalls die Fälle bis zum Verwaltungsgerichtshof sowie Staatsgerichtshof weiterzuziehen. Dieser Trend verdeutlicht die steigende Sensibilität und das gestiegene Bewusstsein der Öffentlichkeit für Datenschutzfragen sowie die zunehmende Bereitschaft, ihre Rechte in diesem Bereich aktiv einzufordern.

Dr. Marie-Louise Gächter, Leiterin Datenschutzstelle

Aus all diesen Gründen war das Berichtsjahr von einem deutlichen gesteigerten Arbeitsaufwand in der DSS geprägt, dem nur dank des Engagements und der Hingabe der Mitarbeiterinnen und Mitarbeiter der DSS erfolgreich begegnet werden konnte. An dieser Stelle möchte ich meinen aufrichtigen Dank für ihren unermüdlichen Einsatz, ihre Fähigkeit, auch in anspruchsvollen Situationen besonnen zu agieren, und ihre Hilfsbereitschaft aussprechen. Ebenso gebührt ein grosses Dankeschön den behördlichen und betrieblichen Datenschutzbeauftragten, mit denen die DSS eng zusammenarbeitet, sowie den engagierten Bürgerinnen und Bürgern, die aktiv ihre Rechte wahrnehmen und Missstände aufzeigen. Ihre Unterstützung und Zusammenarbeit sind von unschätzbarem Wert und tragen massgeblich zum Erfolg unserer Datenschutzarbeit bei.

Vaduz, im April 2024



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

1. Öffentlichkeitsarbeit

Die Öffentlichkeitsarbeit war im Berichtsjahr vor allem von zwei Tendenzen geprägt: Zum einen brachte auch das Jahr 2023 erneut zahlreiche rechtliche und technische Neuerungen, über die von der DSS zu informieren war. Im Vordergrund stand dabei der neue Angemessenheitsbeschluss der Europäischen Kommission für die Vereinigen Staaten von Amerika, das sogenannte Data Protection Framework (DPF). Der Beschluss trat im Juli 2023 in Kraft und sorgte vielerorts für Aufatmen, wenngleich die DSS zu Vorsicht mahnte, denn wie beständig das neue Abkommen sein wird, wird sich erst herausstellen. Auf der anderen Seite zeigte sich aber auch, dass selbst nach sechs Jahren Geltung der DSGVO im Europäischen Wirtschaftsraum nach wie vor Informationsbedarf in Bezug auf Grundwissen herrscht. Dies nicht nur bei neuen Unternehmen oder neu in privaten oder öffentlichen Institutionen tätigen Datenschutzbeauftragten, sondern selbst bei Verantwortlichen, die sich schon lange mit dem Datenschutz beschäftigen. Ein Beispiel war dabei das Auskunftsrecht. Hier sind zwischenzeitlich zahlreiche Unternehmen dazu übergegangen, das Recht auf Kopie in Art. 15 Abs. 3 DSGVO in den Vordergrund zu stellen und etwa Mitarbeitenden vollen Zugriff auf ihre Personalakte zu gewähren oder Kunden auf ihr Kundenkonto. Dabei übersehen sie allerdings, dass sie Art. 15 Abs. 1 DSGVO primär verpflichtet, den betroffenen Personen eine Vielzahl von Informationen zur Verfügung zu stellen, die in einem Personalakt oder einem Kundenkonto nicht ersichtlich sind, wie etwa die Rechtsgrundlage der Verarbeitung, die Speicherdauer und die konkreten Empfänger ihrer Daten.

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 zudem 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, dass eine sehr grosse Zahl an Adressatinnen und Adressaten erreicht werden kann. Die DSS konnte im Berichtsjahr feststellen, dass die Anzahl der Besucherinnen und Besucher der Veranstaltungen erneut deutlich angestiegen ist und wieder das Niveau vor der Corona-Pandemie erreichen konnte bzw. dieses bei einzelnen Veranstaltungen sogar übertraf.

1.1 Veranstaltungen

Der 17. Datenschutztag fand wie üblich zu Beginn des Jahres am 24. Januar im Gemeindesaal Triesen statt. Die DSS lud drei Expertinnen und Experten aus den Bereichen Recht, Wissenschaft und Journalismus ein, um das Thema «Künstliche Intelligenz – Fluch oder Segen?» aus verschiedenen Perspektiven zu beleuchten und zu analysieren. Nach einem fesselnden Einführungsreferat und einer Podiumsdiskussion hatten die Teilnehmenden die Möglichkeit, Fragen zum Thema zu stellen und sich aktiv an der Diskussion zu beteiligen. Während sich bis Anfang des Jahrhunderts fast ausschliesslich nur kleine Gruppen von Forschern, Technikern und spezialisierten Praktikern mit dem Nischenthema Künstliche Intelligenz beschäftigt haben, drängte der rasante Fortschritt diese Technologien in den letzten Jahren immer weiter ins Rampenlicht. Selbstfahrende Autos, Sprachassistenten wie Alexa und Siri, Chatbots und intelligente Telefonsysteme zeigen, dass durch technische Dynamiken unser gesellschaftliches und wirtschaftliches Leben immer mehr von modernster Technologie geprägt sein wird. Hinzu kommen stetig steigende Rechen- wie auch Speicherkapazitäten, welche immer umfangreichere Datenverarbeitungen ermöglichen. Somit verwundert es nicht, dass zahlreiche Fragen einer Beantwortung bedürfen. Welchen Einfluss hat Künstliche Intelligenz bereits und was wird sie noch bringen? Welche weiteren Hürden sind zu bewältigen, wenn Prozesse optimiert und Entscheidungsfindungen vereinfacht werden? Was bedeutet dies für Unternehmen und die öffentliche Verwaltung? Wie wird mit möglichen diskriminierenden Effekten, intransparenten Entscheidungsfindungen und den hohen Energieverbräuchen sowie Treibhausgasemissionen der KI-Modellentwicklung umgegangen? Auch wenn am Datenschutztag nicht alle Fragen abschliessend beantwortet werden konnten, ergaben sich aus den Referaten und Diskussionen zahlreiche Erkenntnisse, aber auch Stoff für weitere Gespräche während dem anschliessenden Apéro und darüber hinaus.

Ebenfalls konnte im Herbst des Berichtsjahres wieder das Vernetzungstreffen für Datenschutzbeauftragte (DSB) stattfinden. Der rege und kontinuierliche Austausch mit den DSB nimmt seit Anfang an einen

hohen Stellenwert in der Tätigkeit der DSS ein. Denn nur so lässt sich erkennen, wo Aufklärungs- und Unterstützungsbedarf besteht. Ebenfalls ist es ein grosses Anliegen der DSS, dass die DSB einen Einblick in die Tätigkeit der Aufsichtsbehörde erhalten. Insbesondere Informationen zu ergangenen Entscheidungen der DSS sorgen für Rechtssicherheit und Orientierungshilfe. Darüber hinaus wies die DSS auch mit einem kurzen Überblick auf relevante Entscheidungen von Aufsichtsbehörden und Gerichten (vor allem) im deutschsprachigen Ausland hin. Auch wenn die DSS an diese Entscheidungen nicht unmittelbar gebunden ist, dienen sie doch einer einheitlichen Anwendung des Datenschutzrechts im EU/EWR-Raum. Die DSS berücksichtigt daher diese Entscheidungen regelmässig in eigenen Verfahren mit. Einen weiteren Schwerpunkt des Treffens bildete ein Überblick über die Ergebnisse einer vom Europäischen Datenschutzausschuss (EDSA) organisierten und koordinierten Umfrage, an der auch die DSS teilnahm und im Rahmen derer sie zahlreiche DSB zu ihren bisherigen Erfahrungen befragte. Wenngleich das Bild in Liechtenstein durchwegs positiv ist und die DSB grundsätzlich mit ihrer Tätigkeit und den zur Verfügung gestellten Rahmenbedingungen recht zufrieden sind, zeigten die Ergebnisse der Umfrage doch auch vereinzelte Schwachstellen auf. Beispielsweise kann die Zugehörigkeit eines DSB zum (höchsten) Management einer Organisation zu Interessenskonflikten führen, wenn ein DSB sowohl über Datenverarbeitungen entscheidet und diese gleichzeitig als DSB frei evaluieren, bewerten und kritisieren sollte. Eine zweite Schwachstelle ergab sich in Bezug auf die Weiterbildung. Ein Drittel der DSB hat maximal einen Tag pro Jahr zum Training und zur Weiterbildung im Datenschutzrecht zur Verfügung. Aus Sicht der DSS wären jedoch mindestens 2 Tage pro Jahr für diesen dynamischen und komplexen Rechtsbereich erforderlich. Gerade auch weil viele DSB diese Aufgabe nicht vollzeitlich ausfüllen, wäre mehr Weiterbildung und Training angemessen, damit sie ihre Organisationen korrekt und mit stets aktuellem Fachwissen beraten können (Art. 38 Abs. 2 DSGVO). Schliesslich stellte sich heraus, dass teilweise vom Management die von den DSB zu erfüllenden Aufgaben (insb. zusätzliche Aufgaben zur DSGVO) zu wenig klar vorgegeben und beschrieben sind. So können potentiell Konflikte entstehen, wenn nicht klar ist, was das Management von einem DSB erwartet und was nicht, und der DSB dies infolgedessen selbst definiert. Ein Konflikt zwischen DSB und Management geht fast immer auf Kosten des Datenschutzes und der Betroffenen. Schlusspunkt der Veranstaltung war ein Vortrag zum neuen Schweizer Datenschutzgesetz und insbesondere seine Bedeutung für Verantwortliche im EWR durch eine Expertin des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in Bern.

Nachdem die DSS auf Grund der Planungsunsicherheit während der Pandemie darauf verzichtet hatte, Workshops durchzuführen, wurde diese im Jahr 2021 eingeführte Veranstaltungsart im Berichtsjahr wieder aufgenommen. Die Wahl des Themas erfolgte auf Grundlage der ernüchternden Erkenntnisse der im Berichtsjahr abgeschlossenen Kontrollen von Unternehmen. Dabei musste festgestellt werden, dass alle gesichteten Datenschutzerklärungen mangelhaft waren. Aufgrund dieser Erkenntnis und den Erfahrungen aus dem Beratungsalltag entschloss sich die DSS, einen Workshop zum Erstellen von Datenschutzerklärungen durchzuführen. Angesichts der grossen Nachfrage erweiterte die DSS dann im September den für einen Tag vorgesehenen Workshop mit dem Titel «Datenschutzerklärung leicht gemacht» auf drei verschiedene Termine. Die hohe Resonanz unterstreicht die wachsende Komplexität, aber auch Relevanz und Bedeutung von Datenschutzerklärungen, die einen entscheidenden Beitrag zur Transparenz und zum Schutz der Privatsphäre leisten und folglich auch häufig Gegenstand von Beschwerden sind.

Am 5. Oktober führte die DSS bereits das zweite Mal einen Anlass im Rahmen der neuen Reihe «Datenschutz goes Cinema» durch. Im Alten Kino Vaduz zeigte sie den Kino-Dokumentarfilm «Coded Bias – Vorprogrammierte Diskriminierung». Anschliessend gab es mit hochrangigen Gästen aus Informatik, Philosophie und Rechtswissenschaft eine Podiumsdiskussion zu Künstlicher Intelligenz, mit welcher das Thema aus verschiedenen Blickwinkeln beleuchtet wurde, insbesondere mit Fokus auf deren Risiken, aber auch Chancen, für Grundrechtsschutz und Privatsphäre. Der Anlass stiess bei der Bevölkerung erneut auf grossen Anklang, weswegen die Veranstaltungsreihe fortgesetzt werden soll.

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.

Auf Einladung der Universität Liechtenstein übernahm die DSS zehn Lektionen im Rahmen des Zertifikationsstudiengangs «Compliance-Officer» im August des Berichtsjahres. 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 Aspekten 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.

Im Rahmen des LL.M. Bank- und Finanzmarktrecht war die DSS verantwortlich für das Thema «Datenschutz und Finanzmarktrecht». In sechs Lektionen stellte die DSS die rechtlichen und technischen Grundlagen des Datenschutzes vor und ging dann auf Fragen ein, die sich aus datenschutzrechtlicher Sicht in Bezug auf die neuen Technologien stellen. Eine der wichtigsten und nach wie vor in der Praxis etwas vernachlässigten Verpflichtungen ist der Grundsatz des Data Privacy by Design and by Default, der seinen Niederschlag in Art. 25 DSGVO gefunden hat. Weitere Schwerpunkte lagen auf der Unterscheidung zwischen Datensicherheit und Informationssicherheit und der Definition des Begriffs Stand der Technik und die Erfordernisse an die Erfüllung dieses Grundsatzes. Schliesslich wurde die Frage des Datenschutzes im Zusammenhang mit der Zahlungsdiensterichtlinie 2 (manchmal abgekürzt als ZaDiRL, meist jedoch PSD 2 von englisch Payment Services Directive), welche Zahlungsdienstleister in der gesamten Europäischen Union (EU) und auch den EFTA/EWR-Staaten einheitlich reguliert, thematisiert.

Am 30. November fand an der Privaten Universität zum wiederholten Mal eine ganztägige Weiterbildungsveranstaltung zum Thema «Datenschutz – Fachwissen für Expertinnen und Experten» statt. Diese Veranstaltungsreihe wird seit nunmehr fünf Jahren von der Privaten Universität im Fürstentum Liechtenstein in Zusammenarbeit mit der Datenschutzstelle, dem Datenschutzverein in Liechtenstein, der Liechtensteinischen Industrie- und Handelskammer, der BWB Rechtsanwälte AG, der Privacyofficers.at und der Data Privacy Community angeboten. Der Vortrag der DSS im Rahmen der im Gemeindesaal Triesen durchgeführten Veranstaltung befasste sich mit dem Thema «Leitlinien des Europäischen Datenschutz-Ausschusses (EDSA)». Die letzten Jahre zeigten, dass die Bedeutung dieser Leitlinien von den Verantwortlichen sehr häufig unterschätzt wird. Dies mag daran liegen, dass sie meist von beträchtlichem Umfang sind und eine gewisse Komplexität aufweisen, die es nicht immer erlaubt, eine Antwort auf eine bestimmte Frage schnell und zweifelsfrei zu identifizieren. Dies ist meist dem Umstand geschuldet, dass die Leitlinien immer auch ein Kompromiss zwischen 30 Aufsichtsbehörden und somit einer Vielzahl von Meinungen sind. Diese Schwierigkeiten nahm die DSS zum Anlass, die für Unternehmen und öffentlichen Stellen in Liechtenstein mutmasslich wichtigsten Leitlinien vorzustellen und die daraus gewonnenen Erkenntnisse für die Praxis verständlich darzulegen.

1.2.2 LLV Kurs – Privatsphäre und Internet/ Smartphone

Wie schon in den Jahren zuvor bot die DSS im Rahmen der internen LLV-Weiterbildung erneut einen Kurs zum Thema «Internet und Privatsphäre» an. Während zwei Vormittagen wurden den Teilnehmenden sowohl Grundsätze als auch Hintergründe zum Schutz des informationellen Selbstbestimmungsrechtes erläutert sowie technisches Wissen im Umgang mit digitalen Endgeräten, insbesondere im Zusammenhang mit dem Schutz der Privatsphäre, nähergebracht. Neben verschiedenen Webbrowsern wurden vor allem die gängigen Betriebssysteme für Smartphones sowie bekannte und viel genutzte Apps analysiert und Möglichkeiten aufgezeigt, wie der Schutz der Privatsphäre durch gezielte Massnahmen bzw. Einstellungen verbessert werden kann. Das Aufzeigen weiterer möglicher Verbesserungsmassnahmen, wie beispielsweise die Verwendung eines Passwortmanagers, die Nutzung einer 2-Faktor-Authentifizierung (2FA) oder ganz allgemein ein sparsamer Umgang mit persönlichen Daten, rundeten den Kurs ab.

1.2.3 Privatschule in Triesen – Cybersicherheit und Cybermobbing

Im Januar 2023 erhielt die DSS eine Anfrage der Fachgruppe Medienkompetenz hinsichtlich eines Workshops für die Privatschule in Triesen. Im Rahmen eines Workshops sollten den Jugendlichen Themenbereiche wie Cybermobbing oder «Das Recht am eigenen Bild» nähergebracht werden. In diesem Zusammenhang wurden auch praktische Tipps sowie Einstellungsmöglichkeiten bei den mobilen Endgeräten erläutert bzw. gemeinsam erarbeitet. Die Jugendlichen zeigten viel Interesse und Engagement während der Veranstaltung. Insbesondere Tipps zu den Einstellungsmöglichkeiten, um beispielsweise Konten auf den Sozialen Medien besser absichern zu können, stiessen auf reges Interesse.

1.2.4 Workshop mit Auszubildenden – Soziale Medien

Im Herbst 2023 zeichnete die DSS verantwortlich für einen Workshop zum Thema «Datenschutz in den sozialen Netzwerken» für die Lernenden des 1. und 2. Lehrjahres einer liechtensteinischen Bank. Da es die DSS als wichtig erachtet, insbesondere auch junge Menschen in Bezug auf datenschutzbezogene Themen zu sensibilisieren, stimmte sie der Durchführung des Kurses gerne zu. Während eines Vormittags wurden die Chancen als auch Risiken im Umgang mit Sozialen Medien gemeinsam mit den Teilnehmenden identifiziert sowie entsprechende Handlungsempfehlungen diskutiert. Als Vorbereitungsauftrag für den Kurs sollten die Teilnehmenden Pro- und Contra-Argumente für die Nutzung von Sozialen Medien ausarbeiten. Somit konnte eine aktive und fruchtbare Diskussion während des Kurses geführt werden. Zusätzlich zeigte die DSS anhand einer Personenrecherche auf, mit welch einfachen Mitteln und Techniken öffentlich zugängliche Informationen gesammelt werden können.

1.2.5 Weitere Vorträge

Zusätzlich zu den erwähnten Veranstaltungen nahmen Mitarbeitende der DSS an 20 weiteren Informations- und Diskussionsveranstaltungen als Referentinnen bzw. Referenten teil oder hielten Vorlesungen oder Vorträge an Informations- und Weiterbildungsveranstaltungen.

Wie bereits in den vergangenen Jahren lud der Schweizer Verein Unternehmens-Datenschutz (VUD) im September des Berichtsjahres die DSS zu einer Veranstaltung in Zürich für betriebliche Datenschutzexperten ein. Diese Veranstaltung im Nachbarstaat stand vor allem im Zeichen der Kooperation der DSS mit Datenschutzbehörden im nahen Ausland sowie dort ansässigen Datenschutzvereinigungen. Gerade mit der Schweiz gibt es zahleiche Anknüpfungspunkte und viele Verantwortliche oder Auftragsverarbeiter in der Schweiz sind entweder direkt der DSGVO unterworfen oder kooperieren mit Unternehmen oder öffentlichen Stellen in Liechtenstein und müssen sich deshalb ebenfalls an die Regeln der DSGVO halten.

Ebenfalls im Zeichen der guten Nachbarschaft stand eine Einladung des Städtebundes Österreichs an die DSS zur Teilnahme an der österreichischen Jahrestagung der Datenschutzbeauftragten des Bundes, der Länder und der Gemeinden im Mai in Graz. Die DSS präsentierte an dieser Tagung das neue EU-U.S. Data Privacy Framework.

Des Weiteren war die DSS im Berichtsjahr mit einem Beitrag zum internationalen Datentransfer am «Privacy Symposium» in Venedig vertreten.

Schliesslich wirkte die DSS auch bei verschiedenen, von Unternehmen ausgerichteten Veranstaltungen mit. Zudem informierte die DSS in Kursen für Gastwirte und Sachbearbeiter/Innen über die grundlegenden Datenschutz-Anforderungen an einen Gastronomie- oder Beherbergungsbetrieb sowie aktuelle Entwicklungen im Bereich Datenschutz.

1.2.6 Schulungen für einzelne Berufsgruppen

Auf Anfrage der Liechtensteinischen Treuhandkammer (THK) präsentierte die DSS die neuesten Entwicklungen im Datenschutzrecht, die von besonderem Interesse für den Treuhandbereich sind. Die Veranstaltung schloss dabei an eine Einführungsveranstaltung der DSS für die Mitglieder der THK im Jahr 2019 an. Gleichzeitig erklärte sich die DSS bereit, die THK bei der Ausarbeitung und Aktualisierung von FAQ im Bereich Treuhandwesen und Datenschutz zu unterstützen.

1.3 Internetseite

Zwei weitere wesentliche Elemente der Öffentlichkeitsarbeit der DSS sind der Internetauftritt sowie der circa alle drei Wochen versandte Newsletter. Die beiden Elemente sind insofern miteinander verbunden, als der Newsletter mit einem kurzen Überblick zu einem bestimmten Thema jeweils auf entsprechende weiterführende Informationen auf der Internetseite verweist.

Die Informationsangebote auf der Internetseite werden laufend erweitert, um Interessierten einfache und praktikable Antworten auf diverse Fragen geben zu können. Dabei werden die Informationen an vielen Stellen mit Beispielen, Mustern und Vorlagen ergänzt, um sowohl verantwortlichen Stellen als auch betroffenen Personen eine effektive und praxisorientierte Unterstützung anbieten zu können. Neu hinzu kamen im Berichtsjahr unter anderem aktuelle Informationen zu den Themen Apple Maps – «Look Around»-Feature in Liechtenstein, Verschlüsselung, Stand der Technik, Künstliche Intelligenz, neuer Angemessenheitsbeschluss der EU-Kommission für die USA (EU-U.S. Data Privacy Framework), neues Datenschutzgesetz in der Schweiz, Chatbots sowie zu Löschrecht und Löschpflicht. Zudem überarbeitete die DSS aufgrund von neuen Entwicklungen in der Praxis, Gesetzgebung, Rechtsprechung oder aufgrund von Leitlinien des EDSA einzelne Themenbereiche und Muster und informierte darüber auch mittels Newsletter.

Die Zugriffe auf die Internetseite stiegen im Berichtsjahr erneut deutlich an. Rund zwei Drittel aller Zugriffe betreffend die verschiedenen Themen unter der Rubrik «Themen A-Z» wurden bei folgenden Beiträgen verzeichnet: Berechtigtes Interesse, besondere

Kategorien personenbezogener Daten nach Art. 9 und personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO, Informationspflicht nach Art. 13 und 14 DSGVO, Chatbots und kleines Konzernprivileg.

1.4 Newsletter

Nach dem Wegfall zahlreicher inaktiver Abonnentinnen und Abonnenten im Rahmen der Umstellung des Newsletter-Systems im Frühjahr 2022, hatten Ende 2023 wieder 950 Personen den Newsletter der DSS abonniert. Dies entspricht einem Plus von 16% gegenüber dem Vorjahr. Das Interesse am Newsletter ist somit nach wie vor ungebrochen. Die Zahl der im Berichtsjahr versandten Newsletter war mit 14 Newslettern etwas geringer als üblich. Die drei meistgelesenen Newsletter 2023 waren die Informationen zum neuen Angemessenheitsbeschluss der EU-Kommission für die USA (EU-U.S. Data Privacy Framework), zur Einführung des «Look-Around»-Features von Apple Maps in Liechtenstein, sowie zum neuen Datenschutzgesetz in der Schweiz.

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 seine Abonnentinnen und Abonnenten immer auf dem Laufenden, auch ohne die Internetseite in regelmässigen Abständen besuchen und auf Neuigkeiten überprüfen zu müssen.

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

1.5 Datenschutz in den Medien

Im Berichtsjahr war der Datenschutz wieder regelmässig in den liechtensteinischen Medien vertreten, wenngleich im Berichtsjahr mit 23 Berichten die Zahl der Berichte etwas zurückging. Die Themen in den Printmedien konzentrierten sich vor allem auf das elektronische Gesundheitsdossier, den Datenschutz im Bildungsbereich, den Austausch von Casino-Sperrlisten oder den seit Juli 2023 wieder zulässigen Datenaustausch mit den USA.

Die Berichterstattung zu datenschutzrechtlichen Themen in den Medien sowie deren positive Haltung gegenüber der Materie ist ein wertvoller Beitrag zum Wissenstransfer datenschutzrechtlicher Themen, da so die Information auch für Personen greifbar wird, die von Berufs wegen weniger Berührungspunkte mit dem Datenschutz haben.

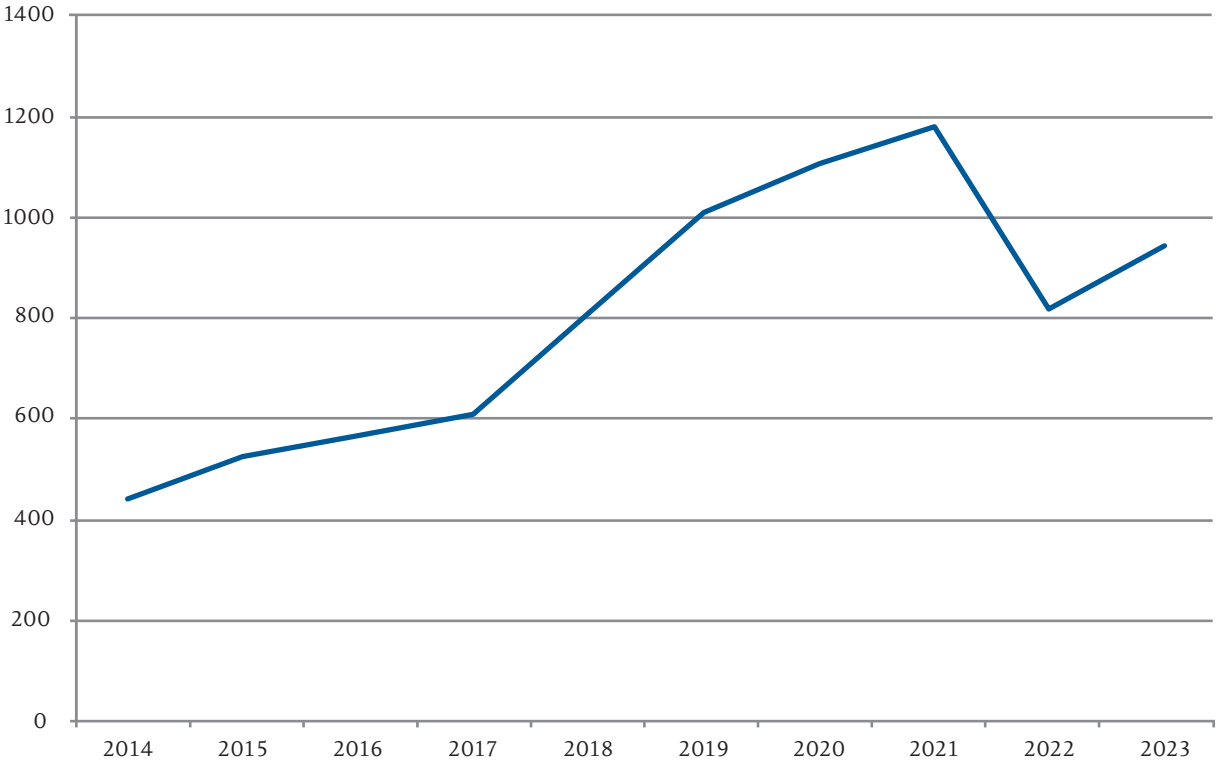


Abbildung 1: Entwicklung Newsletter-Abonnentinnen und Abonnenten

«Privatpersonen machten 12,4 % der Fragestellenden aus und zeigten damit erneut grosses Interesse am Datenschutz.»

2. Beratung zu konkreten Anfragen

2.1 Allgemeines

Im Berichtsjahr erhielt die DSS insgesamt 1'788 Anfragen von öffentlichen und privaten Institutionen sowie Privatpersonen. Im Vergleich zu den im Vorjahr beantworteten 1'503 Anfragen bedeutet dies erneut einen Anstieg um 19%. Über die letzten drei Jahre hinweg zeigt sich zudem eine deutliche Zunahme der Komplexität der Anfragen, ein Trend, der sich auch im Berichtsjahr fortsetzte.

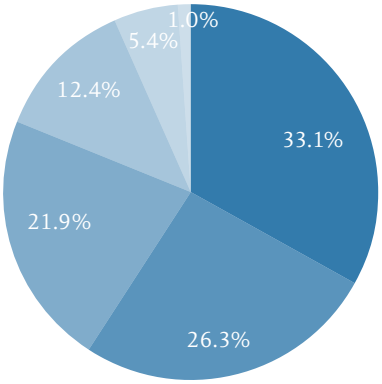
Die fortschreitende technologische Entwicklung brachte eine Vielzahl neuer und anspruchsvoller Fragen hervor, insbesondere im Hinblick auf die Fähigkeit der jeweiligen technischen Systeme, Datenschutzanforderungen zu erfüllen. Besonders die Thematik der künstlichen Intelligenz, vor allem im Kontext von ChatGPT, sorgte bei den Verantwortlichen für zahlreiche Fragen. Darüber hinaus war auch die Beratung zu Fragen rund um den Einsatz von Videoüberwachungsanlagen durch private oder kommerzielle Unternehmen erneut gefragt. Die DSS wurde herausgefordert, vertiefte Informationen im rechtlichen und technischen Bereich bereitzustellen, um umfassende Unterstützung bieten zu können.

In Bezug auf die Herkunft der Fragesteller ist festzuhalten, dass diese dem Trend der letzten Jahre folgend zu einem grossen Teil wieder aus der Privatwirtschaft stammten (33.1%). Der überwiegende Teil der Anfragen kam dabei von KMU-Betrieben diverser Branchen. An zweiter und dritter Stelle folgten internationale Anfragen (26.3%) sowie die Landesverwaltung und die Gemeinden (21.9%). Privatpersonen machten 12.4% der Fragesteller aus, die damit erneut grosses Interesse am Datenschutz zeigten. Die Anfragen von Vereinen und Stiftungen (5.4%) nahmen im Berichtsjahr wieder etwas zu, wohingegen diejenigen von Medien (1.0%) rückläufig waren.

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

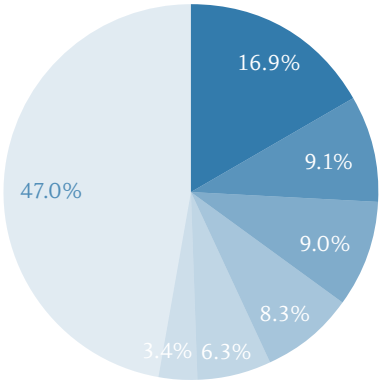
Von den 1'788 Anfragen wurden im Berichtsjahr 232 telefonisch gestellt und beantwortet. Sie stammten von 195 Anrufern, was einer Zunahme im Vergleich zu den Vorjahren entspricht (2022: 144 Anrufer). Erklären lässt sich die Zunahme damit, dass inzwischen zahlreiche Unternehmen und auch öffentliche Stellen in regelmässigem Austausch mit der DSS sind und somit über gute Kontakte mit den Mitarbeitenden der DSS verfügen. In solchen Fällen ist ein Telefonat eine einfache und schnelle Lösung, zumal der Ansprechpartner bzw. die Ansprechpartnerin bei der DSS bereits einen guten Einblick in den datenschutzrechtlichen Alltag der «Stammkunden» hat und weitere Fragen meist einfach und pragmatisch beantworten kann.

Wer stellt die Fragen?



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

Verteilung der Anfragen aus der Privatwirtschaft



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

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 kann».

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 im Berichtsjahr, 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 Neues Datenschutzgesetz in der Schweiz

Am 1. September 2023 sind in der Schweiz das revidierte Datenschutzgesetz und die entsprechende Verordnung in Kraft getreten. Der Datenschutz wird dadurch in der Schweiz gestärkt und die damit zusammenhängenden Pflichten für Datenverarbeiter ähnlich der im EU/EWR-Raum geltenden DSGVO ausgestaltet.

Für liechtensteinische Datenverarbeiter (Verantwortliche und Auftragsverarbeiter), die gezielt Geschäftsbeziehungen in die Schweiz und zu Schweizer Kunden pflegen, bedeutet dies, dass auch sie die neuen Bestimmungen des revidierten Datenschutzgesetzes einhalten müssen. Da sich das neue Schweizer Datenschutzgesetz stark an der DSGVO orientiert und die DSGVO in den meisten Fällen sogar noch leicht strengere Regeln vorsieht, sind für alle Betriebe und Organisationen, welche die DSGVO einhalten, keine zusätzlichen Massnahmen zu ergreifen. Einzig die Datenschutzerklärung sollte um eine präzise Angabe derjenigen Länder ergänzt werden, in die regelmässig Personendaten übermittelt werden. Einen Vertreter in der Schweiz müssen nur solche Datenverarbeiter benennen, welche die sehr eingeschränkten Vorausset-

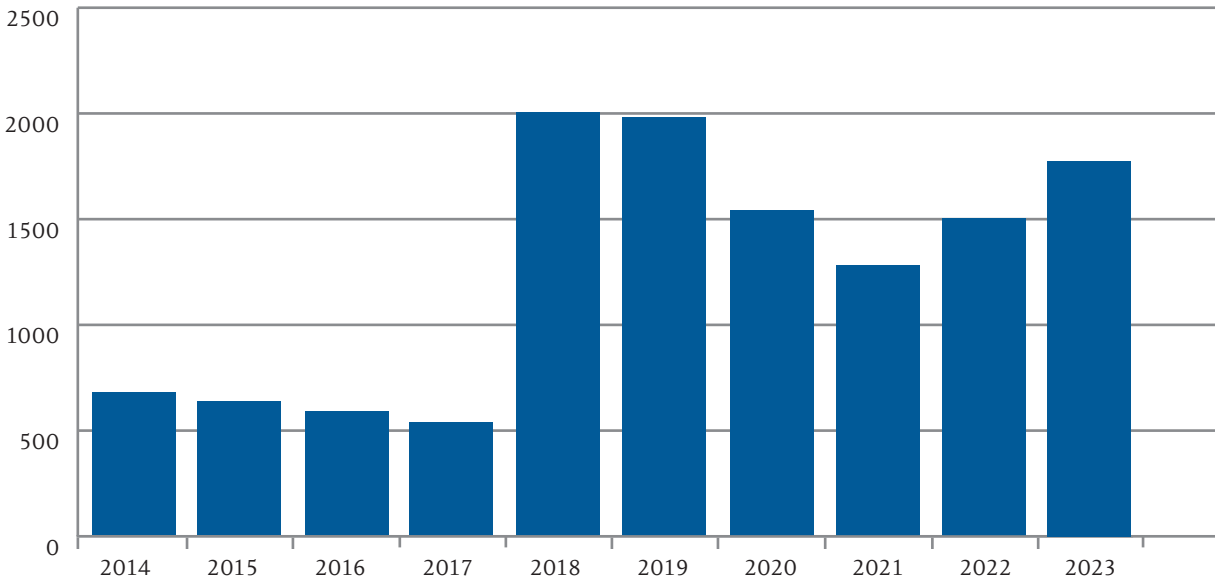


Abbildung 2: Anzahl der Anfragen pro Jahr

zungen von Art. 14 des neuen schweizerischen Datenschutzgesetzes erfüllen. Dies trifft auf die wenigsten liechtensteinischen Betriebe und Organisationen zu. Findet eine Datenschutzverletzung statt, die voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person(en) in der Schweiz zur Folge hat, ist diese nicht nur der DSS, sondern so rasch als möglich auch dem EDÖB zu melden.

Die Schweiz verfügte seit dem Jahr 2000 über einen Angemessenheitsbeschluss der EU, welcher jedoch noch unter der Vorgängerrichtlinie der DSGVO (RL 95/46/EG) erlassen wurde und bis zum Erlass des neuen EU-Beschlusses in Kraft blieb. Mit solch einem Beschluss wird signalisiert, dass das Datenschutzniveau im betreffenden Land gleichwertig wie dasjenige im EU/EWR-Raum ist. Mit Beschluss vom 15. Januar 2024 bestätigte die Europäische Kommission nun die Angemessenheit des Schweizer Datenschutzniveaus, sodass ein ungehinderter Datenfluss von und in die Schweiz weiterhin gewährleistet werden kann.

Für Liechtenstein ist der Angemessenheitsbeschluss für die Schweiz besonders relevant, da ein reger Austausch personenbezogener Daten zwischen Organisationen in den beiden Ländern erfolgt, die Schweiz aus EU/EWR-Perspektive jedoch als Drittland gilt. Die DSS ist daher erleichtert, dass der fragliche Datentransfer in die Schweiz auch künftig ohne grössere Schwierigkeiten erfolgen kann.

2.3 Videoüberwachung und Veröffentlichung von Bildmaterial

Videoüberwachungen sind und bleiben ein aktuelles Thema. Es ist klar erkennbar, dass deren Nutzung stetig weiter ausgebaut wird bzw. werden möchte, und dies in allen Bereichen. Folglich informierte die DSS bereits in den vergangenen Tätigkeitsberichten über den angestiegenen Aufwand an rechtlicher wie auch technisch spezifischer Beratung, welcher dem Trend der stark zunehmenden Nutzung von Videokameras geschuldet ist. Dieser Trend hat nicht nachgelassen und beschäftigt die DSS nach wie vor intensiv. So sind im Berichtsjahr 7 Drohnenflüge mit Kameras und 27 Videoüberwachungsanlagen nach Art. 5 Abs. 7 DSG bei der DSS gemeldet worden. Meldungen von Videoüberwachungen sind immer dann bei der DSS einzureichen, wenn öffentlich zugängliche Räume erfasst werden.

Die Meldungen der Videoüberwachungen erlauben es der DSS, einen Überblick zu erhalten, welche Videoüberwachungen in welchem Umfang zu welchen Zwecken eingesetzt werden. Diese Meldungen werden summarisch geprüft, und es werden stichprobenartig nähere Kontrollen durchgeführt. Bei Auffälligkeiten, wenn zum Beispiel sensible Bereiche betroffen sind, die Anzahl der eingesetzten Kameras oder die Speicherdauer der Aufnahmen auffällig ist, sucht die DSS zunächst das beratende Gespräch, um den Sachverhalt näher zu eruieren, zu klären und gegebenenfalls auf eine datenschutzkonforme Ausgestaltung hinzuwirken. Führt die kooperative Beratung zu keinem aus Sicht des Datenschutzes zufriedenstellenden Ergebnis, wird der hoheitliche Weg beschritten. Neben der Prüfung von eingegangenen Meldungen verfolgt die DSS in Bezug auf Videoüberwachungen vor allem einen beratenden Ansatz, idealerweise bereits vorgängig zu einer Installation bzw. einer Meldung einer Videoüberwachung. In Bezug auf Beratungen, ob in Zusammenhang mit Meldungen oder nicht, musste die DSS im Berichtsjahr in keinem Fall eine Verfügung erlassen. In allen Fällen konnte über den Dialog ein datenschutzkonformes Ergebnis erzielt werden.

Die DSS orientiert sich bei der Beurteilung der Zulässigkeit einer Videoüberwachung an folgenden Grundsätzen: Generell muss die Videoüberwachung objektiv notwendig sein, sprich die Notwendigkeit der Videoüberwachung muss sich aus objektiven Gegebenheiten ableiten lassen. Gemäss deutscher Rechtsprechung kann man eine Videoüberwachung nur dann als objektiv begründbar rechtfertigen, wenn eine Gefährdungslage besteht, die über das allgemeine Lebensrisiko hinausgeht. Eine solche Gefährdung kann sich nur aus tatsächlichen Erkenntnissen ergeben; subjektive Befürchtungen oder ein Gefühl der Unsicherheit reichen hierfür nicht aus. Auch wirtschaftliche oder organisatorische Erwägungen genügen für sich alleine nicht. Weiters muss ein berechtigtes Interesse vorliegen. Während bei Einfamilienhäusern aufgrund der Eigentumsgarantie das berechtigte Interesse von der DSS grosszügig ausgelegt wird und somit Videoüberwachungen des eigenen Grundstücks regelmässig für zulässig befunden werden, ist die Situation anders zu beurteilen, wenn mehrere Parteien, z.B. als Mieter (privat oder geschäftlich) von der Videoüberwachung betroffen sind. In diesen Fällen ist eine objektiv begründbare Notwendigkeit wie auch ein berechtigtes Interesse darzulegen, welches die Interessen der Betroffenen (Mieter, Kunden, Lieferanten, Besucher) überwiegen muss. So sind etwa Videoüberwachungen von Treppenhäusern eines Wohnhauses kritisch zu beurteilen. Handelt es sich dabei noch um Dienstleister im Gesundheitssektor, überwiegen fast ausnahmslos die Interessen der betroffenen Personen. Es müssten besonders triftige Gründe vorgebracht werden, die eine solche Überwachung rechtfertigen.

Nachdem die DSS im Jahr 2020 eine umfassende Kontrolle von Videoüberwachungen in Supermärkten

durchgeführt hat, wurde sie auch im Berichtsjahr wieder insbesondere in Bezug auf neue Supermarktstandorte beratend zur Seite gezogen. Bei der Beratung legt die DSS den Fokus vor allem auf den Schutz der Mitarbeitenden. Kunden befinden sich in der Regel relativ kurz in einem Supermarkt, wohingegen Mitarbeitende einer Videoüberwachung während der gesamten Arbeitszeit ausgesetzt wären. Aus diesem Grunde ist es essenziell, dass die Videoüberwachung nicht flächendeckend eingesetzt, sondern auf die absolut notwendigen und sensiblen Bereiche eingeschränkt wird.

Zusätzlich war die DSS auch im Bereich der staatlichen Videoüberwachung beratend tätig. So wurde die DSS von zwei Gemeinden für eine Beratung bezüglich einer Dokumentation des Baustellenfortschritts kontaktiert. Grundsätzlich empfiehlt die DSS bei Film- und Bildaufnahmen zur Dokumentation von Baustellen die Einstellungen so zu wählen, dass die Erfassung von personenbezogenen Daten verhindert wird. Dies kann etwa durch die Auswahl der Kamera (Weitwinkel), Fokusbereich, Standort, Bildqualität wie auch digitale Massnahmen gewährleistet werden.

Des Weiteren wurde die DSS im Rahmen einer Videoüberwachung eines Gemeindezentrums um datenschutzrechtlichen Rat ersucht. Ein Gemeindezentrum ist ein Begegnungsort, der meist auch zum längeren Verweilen, Austausch und Treffen einlädt. Daher handelt es sich dabei regelmässig um einen Ort der Freizeitgestaltung der Bevölkerung. Eine Überwachung der Freizeitgestaltung von Personen bedarf besonders triftiger Gründe, welche nur in Einzelfällen vorliegen. Gerade für Gemeindezentren in Liechtenstein gilt, dass die Voraussetzungen für eine Videoüberwachung, welche die Freizeitgestaltung der Bürger erfasst, kaum erfüllt werden und eine solche Videoüberwachung somit grundsätzlich unzulässig ist. Da die objektive Notwendigkeit einer Videoüberwachung aufgrund von Vorfällen meist insbesondere für die Zeit der Dämmerung und nachts gegeben ist, kann eine Videoüberwachung zu diesen Zeiten jedoch zulässig sein. Zentral dabei ist eine transparente Information der Bevölkerung, welche auch die zeitliche Einschränkung der Videoüberwachung klar kommuniziert.

Wie im letzten Tätigkeitsbericht bereits ausführlich erläutert, war die DSS bei der Umsetzung der landespolizeilichen Videoüberwachung in Schaan (beim Busplatz, beim Lindaplatz, beim SAL, an der Kreuzung neben dem Postgebäude wie auch an der Kreuzung nach Nendeln) beratend tätig. Ende 2022 wurde die Videoüberwachung operativ. Wie die DSS im Tätigkeitsbericht 2022 ausführte, war zu diesem Zeitpunkt eine Information über die wesentlichen Eckpunkte der Videoüberwachung sowie eine weitergehende spezifische Information gemäss Art. 13 DSGVO auf der Internetseite der Landespolizei noch ausstehend. Auch im Berichtsjahr wurde dieser Mangel nicht behoben.

Des Weiteren wurde die DSS in Zusammenhang mit Videoüberwachungen bei einem Musikfestival, in einem Schwimmbad, Hofladen, Casino, in Unternehmen, Parkhäusern, Ämtern und zur Schneeräumung beratend tätig. Dies zeigt wie vielfältig der Einsatz von Videoüberwachung ist und wie umfassend die Beratung der DSS diesbezüglich ausfällt.

Aufgefallen ist der DSS im Rahmen ihrer beratenden Tätigkeit, dass das Erstellen eines klaren und informativen Piktogramms einigen Verantwortlichen schwerfällt. Trotz der umfassenden Hilfestellungen inklusive Muster und Vorlage, welche die DSS zur Verfügung stellt, ergeben sich immer wieder Fragen und Unklarheiten. Daher hat die DSS die diesbezügliche Beratung weiter verstärkt und bietet an, einen Entwurf vor dessen Druck und Anbringung zu sichten, zu kommentieren und allenfalls zu korrigieren.

Beschwerden in Bezug auf Drohnen, die unbefugt und entgegen dem Datenschutz über private Gärten, Terrassen und Balkone fliegen und dabei Bild- oder Videoaufnahmen anfertigen, sind im Berichtsjahr keine eingegangen. Drohnenpiloten sind zunehmend sensibilisiert, wohl auch durch die gestiegenen Anforderungen im In- und Ausland (z.B. Pilotenschein). Es erfolgten allerdings einige Beratungsanfragen an die DSS bezüglich der Zulässigkeit von Drohnenflügen wie auch zu den Meldungen nach Art. 5 Abs. 7 DSG. Touristen, Blogger und Fotografen kontaktierten die DSS vor ihrem Besuch bzw. dem Drohnenflug und erkundigten sich über die lokalen datenschutzrechtlichen Spezifitäten und Voraussetzungen.

2.4 Verbindliche interne Datenschutzvorschriften

Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules; BCR) sind eine Möglichkeit unter dem Kapitel V der DSGVO, einen sicheren Datentransfer in Drittstaaten zu gewährleisten. Sie bieten sich insbesondere für weltweit tätige Unternehmen mit zahlreichen Tochtergesellschaften in verschiedenen Ländern an. Sie dienen dazu, den Datenschutz auf Datenverarbeitungen auszuweiten, im Rahmen derer personenbezogene Daten vom EU/EWR-Raum aus in Drittländer gelangen.

Bereits vor Geltung der DSGVO wurde das Konzept der BCR geschaffen und laufend verfeinert. Aufgrund des Erfolges wurde es mit der DSGVO «verrechtlicht» und nochmals konkretisiert. BCR bieten den 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.

Die DSGVO sieht vor, dass es für 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, welche eine Anleitung für Antragsteller bieten und Inhalte 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 Diskussionspunkte von allen europäischen Behörden abschliessend behandelt werden.

Die vom EDSA ausgearbeiteten Leitlinien wurden von der «International Transfer Subgroup» im Rahmen von langen und intensiven Diskussionen überarbeitet. Dabei wurden alle Erfahrungen der EWR-Mitgliedstaaten in Zusammenhang mit BCR-Genehmigungsverfahren zusammengetragen diskutiert und als einheitliche Leitlinie für alle festgehalten. Diese wurde im Berichtsjahr der öffentlichen Vernehmlassung zugänglich gemacht, nochmals überarbeitet und präzisiert und schliesslich im Sommer des Berichtsjahres abgeschlossen. Diese Leitlinie ist das Herzstück für jede Ausarbeitung von verbindlichen internen Datenschutzvorschriften für Verantwortliche.

Ein schon länger aktuelles und viel diskutiertes Thema der Aufsichtsbehörden ist die Arbeitslast wie auch die grosse Anzahl der 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 wird. Diese Schritte wurden bisher nacheinander durchgeführt. Durch die Parallelität verspricht man sich nicht nur Zeitersparnisse, sondern auch einen intensiveren und ergebnisorientierteren Austausch bezüglich offener Fragen zwischen den überprüfenden Behörden. Weiters fiel im Berichtsjahr die Entscheidung, EDSA-intern die Ausarbeitung eines Prozesses zur Begleitung der Genehmigungsverfahren zu lancieren.

Wie im letzten Tätigkeitsbericht ausgeführt, ist seit 2022 bei der DSS das zweite BCR-Verfahren anhängig. Im Berichtsjahr konnten das Co-Review-Verfahren abgeschlossen und im Kooperationsverfahren bis auf einen alle offenen Punkte geklärt werden. Bei dem nach wie vor ungeklärten Punkt geht es um die Frage, wie die Besonderheit berücksichtigt werden kann, dass die BCR gleichzeitig die unternehmensinterne Datenschutzrichtlinie darstellen. Ebenso bleibt zu klären, wie eine Genehmigung in anderen Ländern (wie etwa der Türkei, der Schweiz oder Grossbritannien) angestrebt werden kann. Diese Fragestellung wird voraussichtlich von der DSS am nächsten BCR-Workshop im Jahr 2024 als Inputthema vorgestellt werden.

2.5 Auswahl konkreter rechtlicher Fragen

Übermittlung von Mitarbeiterdaten an Polizeibehörden im Zusammenhang mit Verkehrsbussen in Firmenfahrzeugen

Ein Liechtensteiner Unternehmen wandte sich zur Überprüfung der Datenschutzkonformität des folgenden Verarbeitungsprozesses an die DSS: Die Abwicklung von Verkehrsbussen, die Mitarbeitende während der Nutzung von Dienst- oder Firmenwagen verursacht hatten, sollte verbessert werden. Anstatt die Aufforderung zur Bezahlung der Verkehrsbusse von der Behörde zu erhalten und unternehmensintern an die betroffenen Mitarbeitenden weiterzuleiten, die in einem weiteren Schritt ihre Lenkerdaten an die Behörden übermitteln mussten, wollte das Unternehmen die Mitarbeiterdaten direkt an die jeweilige Behörde übermitteln. Mit dieser Änderung sollten arbeits- und kostenintensive Verzögerungen und Mahngebühren reduziert werden.

Als Rechtsgrundlage für die Weitergabe dieser personenbezogenen Daten wurden Art. 6 Abs 1. Bst. f DSGVO und alternativ oder ergänzend Bst. c vorgeschlagen. Art. 6 Abs. 1 Bst. c DSGVO beschreibt die Datenverarbeitung aufgrund einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt. Das Unternehmen erhält in seiner Eigenschaft als Fahrzeughalter die Aufforderung zur Bekanntgabe der Lenker-Daten von den Behörden und darf/muss in Erfüllung der rechtlichen Pflicht die Lenker-Daten an die Behörden übermitteln. Diese rechtliche Verpflichtung ergibt sich aus dem Unionsrecht oder dem Recht der Mitgliedsstaaten aus dem EU/EWR-Raum. Eine direkte Übermittlung an die Behörden ist somit zulässig.

Für Behörden aus Drittstaaten wie etwa der Schweiz ist dies mangels einer Rechtsgrundlage im EU/EWR-Raum nicht zulässig und es kann stattdessen das berechtigte Interesse des Unternehmens gemäss Art. 6 Abs. 1 Bst. f DSGVO herangezogen werden. Zu beachten ist im Fall des Bst. f indes, dass eine betroffene Person aus Gründen, die sich aus ihrer besonderen Situation ergeben, ein Widerspruchsrecht gemäss Art. 21 DSGVO hat.

Remote Work in einem Drittstaat
Ein Unternehmen erkundigte sich bei der DSS, ob ein Mitarbeitender des Unternehmens, der sich in einem Drittstaat aufhält und remote arbeitet, als Auftragsverarbeiter einzustufen sei und welche datenschutzrechtlichen Massnahmen sich daraus ergäben.

In den Guidelines des EDSA zum Zusammenspiel zwischen der Anwendung des Art. 3 DSGVO und den Bestimmungen zu Drittstaatentransfer nach Kapitel V DSGVO (EDPB Guidelines 05-2021) wird der Fall des Unternehmensmitarbeiters im Drittstaat geregelt. Für einen Datentransfer in einen Drittstaat müssen personenbezogene Daten von einem Verantwortlichen oder Auftragsverarbeiter an einen anderen, vom ersten verschiedenen Verantwortlichen oder Auftragsverarbeiter übermittelt werden. Der Mitarbeiter und das Unternehmen sind jedoch nicht als separate Akteure zu betrachten, daher gilt der interne Datenaustausch auch nicht als Datentransfer in einen Drittstaat. Ein Datentransfer würde erst vorliegen, wenn der Mitarbeitende Daten an Dritte weitergeben oder als eigene rechtliche Tochtergesellschaft auftreten würde. Für Mitarbeitende im Home-Office und allgemein beim Remote-Zugriff ist allerdings zu beachten, dass die betroffenen Daten und Geräte durch angemessene technische und organisatorische Massnahmen (TOMs) geschützt sind.

Erstellung von Audiodateien in einem Mietverhältnis
Die DSS wurde von einer Privatperson kontaktiert, die sich als Mieterin vom Lärm aus einer benachbarten Wohnung gestört fühlte. Sie wollte wissen, ob es rechtlich erlaubt sei, zu Dokumentationszwecken Tonaufnahmen der Geräusche etc. zu machen und diese dann der Hausverwaltung zu übergeben. Tonaufnahmen können in Verbindung mit Namen und Wohnungsadresse als personenbezogene Daten zu klassifizieren sein und eine Weitergabe an die Hausverwaltung stellt folglich eine Datenverarbeitung nach der DSGVO dar. Für die Weitergabe an die Hausverwaltung wäre die Einwilligung der aufgenommenen Nachbarn notwendig, mit der in der Praxis aller Wahrscheinlichkeit nach nicht zu rechnen ist. Als rechtlich zulässige Alternative bietet sich ein schriftliches Protokoll der Geräusche für die Beschwerde an die Hausverwaltung an, dieses gilt nicht als Verarbeitung personenbezogener Daten, sondern als Aussage.

Löschung von Kundenkonten eines Online-Shops
Ein Online-Shop wandte sich mit der Frage an die DSS, ob den Kunden die Möglichkeit zur Löschung ihrer Kundenkonten geboten werden müsste und ob diesbezüglich ein Zeitraum vorgegeben ist.

Art. 17 Abs. 1 DSGVO räumt allen von der Verarbeitung personenbezogener Daten betroffenen Personen das Recht ein, die Daten vom Verantwortlichen löschen zu lassen, wenn bestimmte Voraussetzungen erfüllt sind. Ist die Verarbeitung aufgrund der Einwilligung der betroffenen Person erfolgt, wie im Fall der Kundenkonten, hat der Verantwortliche bei Widerruf der Einwilligung die Daten unverzüglich zu löschen. Die Art der Löschung, also ob der Kunde selbst oder das Unternehmen auf Anfrage des Kunden die Löschung vornimmt, ist nicht vorgegeben, es muss nur die Möglichkeit zur Löschung bestehen.

Gewisse personenbezogene Daten werden gemäss Art. 17 Abs. 3 Bst. b DSGVO allerdings von der Unverzüglichkeit der Löschpflicht ausgenommen, da sie zur Erfüllung einer gesetzlichen Verpflichtung notwendig sind und während der gesetzlich bezeichneten Frist gespeichert werden dürfen/müssen (bspw. Belege für die Buchhaltung oder die Erfüllung allfälliger Gewährleistungsrechte).

Selbstjustiz auf der Basis von Videoaufzeichnungen durch Hochladen derselben in den sozialen Medien
Von Seiten der Medien erreichte die DSS die Anfrage, ob ein Unternehmen, das zu Zwecken der Aufklärung von Diebstählen eine Videoüberwachung sensibler Bereiche einsetzte, bei einem effektiv erfolgten Diebstahl die diesbezüglichen Videoaufzeichnungen auf YouTube stellen darf.

Die DSS informierte hierzu, dass für die Verfolgung und Aufdeckung von Delikten nicht Unternehmen zuständig sind. Dies selbst dann nicht, wenn sie Geschädigte von Delikten sind. Zuständig hierfür sind die Strafverfolgungsbehörden. Der einzig richtige Weg für ein Unternehmen bei einem Einbruch ist damit die Meldung des Deliktes an die zuständige Strafverfolgungsbehörde (Landespolizei). Im Rahmen der Verfolgung und Aufdeckung des Deliktes wird die Landespolizei auch die Videoaufzeichnungen sichten.

Aus datenschutzrechtlicher Sicht bedarf es für jede Datenverarbeitung eines Rechtfertigungsgrundes gemäss Art. 6 Abs. 1 DSGVO. Einen solchen Rechtfertigungsgrund hatte das betreffende Unternehmen bei der Veröffentlichung von Fotos von der eigenen Überwachungskamera auf den sozialen Medien nicht.

Zweck von Videoüberwachungen in Geschäften ist zwar gerade die Sicherung von Beweisen bei Diebstählen und somit lag für die Videoaufnahme als solche sowie die Weitergabe der Aufnahmen an die Polizei ein Rechtfertigungsgrund vor. Keinen Rechtfertigungsgrund hatte das Unternehmen jedoch für die Offenlegung der Fotos des mutmasslichen Diebes auf den sozialen Medien.

Kündigungs- / Abberufungsschutz des Datenschutzbeauftragten

Von Seiten eines Datenschutzbeauftragten erreichte die DSS die Anfrage zum Abberufungsschutz des Datenschutzbeauftragten. Art. 38 Abs. 3 DSGVO sieht vor, dass ein Datenschutzbeauftragter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden darf. Nicht selten erfolgt eine Verwechslung von Abberufungs- und Kündigungsschutz, die aber nicht gleichzusetzen sind. Das deutsche BDSG hat mit Verweis auf § 6 Abs. 4 BDSG in dessen § 38 Abs. 2 BDSG eine Regelung geschaffen, die einen Kündigungsschutz für den betrieblichen Datenschutzbeauftragten im nicht-öffentlichen Bereich enthält. Während der Amtszeit als betrieblicher Datenschutzbeauftragter im nicht-öffentlichen Bereich und bis ein Jahr nach Beendigung der Funktion als Datenschutzbeauftragter ist nach dieser Bestimmung eine Kündigung des Arbeitsverhältnisses nur möglich, wenn der Arbeitgeber zur fristlosen Kündigung berechtigt ist. Aus welchen Gründen die Beendigung der Amtszeit als Datenschutzbeauftragter erfolgte, ist hierbei nicht entscheidend. Als Gründe kommen gleichermassen die Niederlegung des Amtes durch den betrieblichen Datenschutzbeauftragten, die einvernehmliche Aufhebung oder der Untergang des Rechtsträgers durch Verschmelzung in Betracht. Liechtenstein hat diese Bestimmung nicht ins nationale DSG übernommen, womit die Schutzfrist von einem Jahr in Liechtenstein für betriebliche Datenschutzbeauftragte im nicht-öffentlichen Bereich nicht gilt und allein die allgemeinen arbeitsrechtlichen Bestimmungen von § 1173a ABGB massgebend sind.

Aufnahme von Telefonaten

Wiederkehrend waren auch dieses Jahr Fragen zu den Möglichkeiten und Erfordernissen der Aufnahme von Telefonaten. Der Gedanke der Aufnahme von Telefonaten zu Schulungs-, Qualitätssicherungs- und Beweiszwecken mag durchaus verlockend sein, doch so ganz einfach gestaltet sich die Realisierung eines solchen Vorhabens nicht. Von ganz wenigen Ausnahmen abgesehen, so etwa dann, wenn gesetzliche Vorgaben den Verantwortlichen zur Aufnahme von Telefonaten legitimieren (z.B. Vorgaben aus MIFID II), bedarf es für die Aufnahme von Telefonaten einer Einwilligung, welche die Bedingungen gemäss Art. 7 DSGVO zu erfüllen hat. In Entsprechung hiervon muss der Anrufende vor Beginn der Telefonaufzeichnung gefragt werden, ob er mit der Telefonaufzeichnung einverstanden ist und dies im Falle seines Einverständnisses durch eine aktiv bestätigende Handlung wie dem Aussprechen eines «Ja» oder der Wahl einer vorgegebenen Telefontaste bestätigen. Keine wirksame Einwilligung wäre damit die blosse Einräumung einer Widerspruchsmöglichkeit mit nachfolgender Fortsetzung des Telefonats. Als Folge der Rechenschaftspflicht gemäss Art. 5 Abs. 2 DSGVO obliegt es dem Verantwortlichen zu beweisen, dass die betroffene Person die Einwilligung gemäss Art. 7 DSGVO «in informierter Weise» erteilt hat. Dieses Vorgehen entspricht auch den Empfehlungen der Datenschutzkonferenz (DSK), dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder. Neben den deutschen Datenschutzaufsichtsbehörden wird diese Einschätzung auch von zahlreichen weiteren Datenschutzaufsichtsbehörden der EWR/EU-Mitgliedstaaten vertreten.

Keinesfalls genügend ist damit die Heranziehung der berechtigten Interessen gemäss Art. 6 Abs. 1 Bst. f DSGVO, fehlt es doch regelmässig an der Erforderlichkeit. Überdies stehen gewichtige Interessen der betroffenen Person einer solchen Telefonaufzeichnung entgegen. Im Besonderen angesprochen ist hier die Sicherstellung der Vertraulichkeit des nicht-öffentlichen Worts. Nicht anders verhält es sich mit der Aufzeichnung von Telefonaten zu Schulungszwecken. Auch hier besteht in aller Regel keine Erforderlichkeit. Vielmehr kann der mit der Telefonaufzeichnung intendierte Zweck in gleicher Weise erreicht werden durch das Nachstellen typischer Gesprächssituationen. Und auch für Beweissicherungszwecke ist Art. 6 Abs. 1 Bst. f DSGVO in aller Regel keine Rechtsgrundlage, da es mildere, weniger stark in die Persönlichkeitsrechte der betroffenen Person eingreifende Möglichkeiten gibt.

Soweit es keine gesetzliche Pflicht zur Aufzeichnung gibt, ist somit festzuhalten, dass die Einwilligung der betroffenen Person, welche die Bedingungen gemäss Art. 7 DSGVO erfüllt, die einzige Rechtsgrundlage ist, auf welche Telefonaufzeichnungen gegründet werden können.

Offenlegung von Lohndaten an Stiftungsrat

Die DSS hatte sich mit der Zulässigkeit der Offenlegung von Lohndaten, wie Lohn, Mitarbeitergespräche und Lohnerhöhungen von einer Geschäftsstelle gegenüber einem Stiftungsrat zu befassen. Dabei ist grundsätzlich festzuhalten, dass für die strategische Führung grundsätzlich keine detaillierten Kenntnisse über Lohndaten erforderlich sind. Dennoch kann es unter gewissen Voraussetzungen zulässig und erforderlich sein, dass ein Stiftungsrat Kenntnis über Lohndaten erhält. Zentral ist dabei die klare Zuteilung von Kompetenzen und Aufgaben, um bestimmen zu können, ob eine Datenverarbeitung für die Erledigung der Aufgaben erforderlich ist. Daher ist es ratsam, diese in Statuten oder anderen internen Reglementen klar zu definieren. Weiters sind die Umstände des jeweiligen

Einzelfalles zu beurteilen. So kann die Kenntnis/Verarbeitung von Lohndaten beispielsweise für einen Stiftungsrat erforderlich sein, um die strategische Weiterentwicklung zu definieren oder wichtige Personalentscheidungen zu treffen. In diesem Zusammenhang kann eine einmalige Offenlegung im Einzelfall zulässig sein. Sollte eine regelmässige Offenlegung vorgesehen sein, hängt dies von den internen Regelungen und Kompetenzen ab und sollte im besten Fall klar definiert sein. In jedem Fall handelt es sich jedoch um eine Einzelfallbeurteilung.

2.6 Auswahl konkreter technischer Fragen

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

DSGVO-Konformität bestimmter KI-gestützter Online-Dienste

Die Zahl der Nutzer von KI-basierten Online-Diensten steigt ebenso wie die Zahl der öffentlich verfügbaren Dienste kontinuierlich an. Insbesondere sogenannte generative KI-Technologien (z.B. Chat-GPT von OpenAI und LaMDA (Google Bard)) haben jüngst innerhalb kürzester Zeit grosse Aufmerksamkeit und Popularität erlangt. Mit der weiteren Verbreitung dieser Technologien rücken auch die mit ihrem Einsatz verbundenen Datenschutzfragen immer mehr in den Vordergrund. Im Jahr 2023 erhielt die DSS mehrere Anfragen von Unternehmen zur Einhaltung der DSGVO bei der Nutzung von KI-gestützten Online-Diensten. Bei diesen Anfragen zur Datenverarbeitung im Zusammenhang mit KI-Technologien ging es häufig um die Ausgestaltung der Informationen nach Art. 13 DSGVO, die damit verbundenen Datenübermittlungen in Drittstaaten, die notwendige Wahl der richtigen Rechtsgrundlage, die damit verbundene Verarbeitung von Telemetriedaten und auch um die Frage, ob die DSS selbst Erfahrungen mit bestimmten KI-gestützten Diensten hat. Zusammenfassend lässt sich festhalten, dass der Einsatz von KI-gestützten Online-Diensten nicht grundsätzlich unzulässig oder mit dem Datenschutz unvereinbar ist. Vielmehr kommt es auf den konkreten Einzelfall und insbesondere auf die verarbeiteten personenbezogenen Daten an. Hervorzuheben ist in diesem Zusammenhang, dass der Einsatz von KI-Technologien aus datenschutzrechtlicher Sicht derzeit noch mit zahlreichen Rechtsunsicherheiten behaftet ist. Dies betrifft beispielsweise bei (generativen) KI-Technologien insbesondere die Erhebung personenbezogener Daten aus öffentlich zugänglichen Quellen, die Verwendung dieser personenbezogenen Daten als Trainingsdaten im Rahmen des maschinellen Lernens, die Speicherung personenbezogener Daten als Folge des maschinellen Lernens und die Verarbeitung personenbezogener Daten der Nutzerinnen und Nutzer. Erschwerend kommt in diesem Zusammenhang hinzu, dass Nutzerinnen und Nutzer in der Regel technisch nicht daran gehindert werden können, personenbezogene und sensible Daten an KI-Systeme zu übermitteln.

Besonderheiten bei der korrekten Umsetzung von Löschfristen bei der Veröffentlichung personenbezogener Daten im Internet

In Zeiten fortschreitender Digitalisierung werden immer mehr personenbezogene Daten im Internet veröffentlicht. Dies geschieht auch im Rahmen der Erfüllung amtlicher Aufgaben, wie etwa der Publikation amtlicher Kundmachungen durch öffentliche Stellen. Im Rahmen ihrer Tätigkeit war die DSS im Berichtsjahr mehrfach mit der Thematik der Löschung von im Internet veröffentlichten personenbezogenen Daten konfrontiert. Dabei stellte die DSS insbesondere fest, dass es bei im Internet veröffentlichten Daten immer wieder zu Verstössen bei der Einhaltung der Löschfristen kommt. Dies ist häufig darauf zurückzuführen, dass vergessen wird, die fraglichen Dokumente von den ursprünglichen Veröffentlichungsquellen zu löschen. Häufig existieren zudem Kopien der entsprechenden Dokumente, die auch nach der Löschung auf den ursprünglichen Servern noch einige Zeit in den öffentlich zugänglichen Suchergebnislisten gängiger Suchmaschinen (wie Google oder Bing) auftauchen. Für Verantwortliche ist es daher wichtig, Prozesse zu etablieren, die sicherstellen, dass die Löschfristen auch für im Internet veröffentlichte personenbezogene Daten eingehalten werden. Darüber hinaus stellen alle gängigen Suchmaschinen entsprechende Handlungsanweisungen zur Entfernung veralteter Inhalte zur Verfügung. So ist es in den meisten Fällen möglich, durch Ausfüllen eines Online-Formulars Löschanträge an die Suchmaschinenbetreiber zu übermitteln, wodurch entsprechende Dokumente nach einer Prüfung dauerhaft aus den Suchergebnislisten entfernt werden. Umfassende Informationen zum Thema Löschrecht und Löschpflicht stellt die DSS auf ihrer Internetseite zur Verfügung.

Content Delivery Network (CDN) Dienste

Aufgrund der komplexen Datenverarbeitungen und vielfältigen Dienstleistungsangebote im Rahmen der Nutzung von sogenannten CDN Diensten erreichen die DSS häufig Anfragen zur «DSGVO-Konformität». Grundsätzlich sind bei einer Nutzung eines CDN-Dienstes, sofern der sachliche Anwendungsbereich gemäss Art. 2 DSGVO erfüllt ist, die datenschutz-

rechtlichen Anforderungen zu erfüllen. Aufgrund der verschiedenen Anbieter und Funktionen bzw. IT-Sicherheitslösungen, die angeboten werden, lässt sich pauschal allerdings nicht beantworten, ob eine Nutzung DSGVO-konform ist oder nicht. Erschwerend hinsichtlich der Beurteilung kommen verschiedene Konfigurationsmöglichkeiten der Dienste – im Zusammenhang mit den konkreten Anforderungen des Unternehmens – hinzu. Deshalb ist meistens eine Einzelfallprüfung unabdingbar. Als Startpunkt für eine solche Überprüfung eignet sich die Sichtung der Datenschutzerklärung des Anbieters.

2.7 Wichtigste EuGH-Entscheidungen 2023

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, wurde entschieden, auf die bedeutendsten Entscheidungen in diesem Bericht hinzuweisen.

EuGH, 12. Januar 2023, C-154/21: Österreichische Post (Informationen über die Empfänger personenbezogener Daten)

Der EuGH hat entschieden, dass der Auskunftsanspruch aus Art. 15 Abs. 1 Bst. c DSGVO regelmässig auch die Identität der Empfänger personenbezogener Daten umfasst. Nur wenn es (noch) nicht möglich ist, diese Empfänger zu identifizieren, kann sich der Verantwortliche darauf beschränken, lediglich die Kategorien der betreffenden Empfänger mitzuteilen. Dies ist ebenfalls der Fall, wenn der Verantwortliche nachweist, dass der Antrag offenkundig unbegründet oder exzessiv im Sinne von Art. 12 Abs. 5 DSGVO ist.

EuGH, 30. März 2023, C-34/21: Hauptpersonalrat der Lehrerinnen und Lehrer (Beschäftigtendatenschutz)

Zunächst stellt der EuGH fest, dass die Verarbeitung personenbezogener Daten von Lehrkräften beim Videokonferenz-Livestream des von ihnen erteilten öffentlichen Schulunterrichts in den sachlichen Anwendungsbereich der DSGVO fällt. Er stellt sodann klar, dass diese Verarbeitung der personenbezogenen Daten von Lehrkräften, die als Angestellte oder Beamte im öffentlichen Dienst stehen, in den sachlichen und persönlichen Anwendungsbereich des Art. 88 DSGVO fällt, der auf die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext abstellt.

Art. 88 DSGVO ist dahin auszulegen, dass eine nationale Rechtsvorschrift keine «spezifischere Vorschrift» im Sinne von Abs. 1 dieses Artikels sein kann, wenn sie nicht die Vorgaben von Abs. 2 dieses Artikels erfüllt.

Der Gerichtshof stellt überdies klar, dass nationale Rechtsvorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten von Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext unangewendet bleiben müssen, wenn sie nicht die in Art. 88 Abs. 1 und 2 DSGVO vorgegebenen Voraussetzungen und Grenzen beachten, es sei denn, die in Rede stehenden Rechtsvorschriften stellen eine Rechtsgrundlage für die Verarbeitung im Sinne von Art. 6 Abs. 3 DSGVO dar, die den Anforderungen dieser Verordnung genügt.

Dieses Urteil hat auf Liechtenstein nur mittelbare Auswirkung, da Liechtenstein kein eigenständiges Gesetz zum Thema erlassen hat. Stattdessen gelten einige spezielle Normen, die sich auf die Datenverarbeitung im Beschäftigungsverhältnis beziehen (z.B. Art. 26 Datenschutzgesetz (DSG), §1173a Art. 27 und 28a Allgemeines bürgerliches Gesetzbuch (ABGB), Art. 59 Verordnung I zum Arbeitsgesetz (ArGV I)). Darüber hinaus kommen auch weitere Normen des Grundrechts- und Persönlichkeitsschutzes zur Anwendung (z.B. Art. 3, 8 und 13 Gleichstellungsgesetz (GLG), Art. 39 Personen- und Gesellschaftsrecht (PGR)).

EuGH, 4. Mai 2023, C-487/21: Österreichische Datenschutzbehörde und CRIF (Recht auf Kopie)

Der EuGH stellt fest, dass das Recht auf Kopie nach Art. 15 Abs. 3 DSGVO die originalgetreue und verständliche Reproduktion der personenbezogenen Daten des Betroffenen umfasst. Dieses Recht umfasst die Befugnis, eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die unter anderem diese Daten enthalten, zu erlangen, wenn die Zurverfügungstellung einer solchen Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch diese Verordnung verliehenen Rechte zu ermöglichen, freilich immer unter Berücksichtigung der Rechte und Freiheiten anderer.

Art. 15 Abs. 3 Satz 3 DSGVO ist dahin auszulegen, dass sich der im Sinne dieser Bestimmung verwendete Begriff «Informationen» ausschliesslich auf personenbezogene Daten bezieht, von denen der für die Verarbeitung Verantwortliche gemäss Satz 1 dieses Absatzes eine Kopie zur Verfügung stellen muss.

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, 4. Mai 2023, C-300/21: Österreichische Post (Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten)

In einem weiteren Urteil hat sich der EuGH mit dem Recht auf Schadenersatz nach Art. 82 DSGVO auseinandergesetzt. Der EuGH betont, dass die Begriffe des materiellen und immateriellen Schadenersatzes als autonome Begriffe des Europarechts in allen Mitgliedsstaaten einheitlich auszulegen sind. Voraussetzung für einen Schadenersatzanspruch ist, dass ein Schaden eingetreten ist, der kausal auf einem Verstoss gegen die DSGVO beruht. Daraus folgt, dass nicht jeder Verstoss gegen die DSGVO automatisch zu einem Schadenersatzanspruch führt.

Eine Erheblichkeitsschwelle, so der EuGH, muss nicht erreicht werden, um Anspruch auf einen immateriellen Schadenersatz zu haben. In der DSGVO wird ein solches Erfordernis nicht erwähnt und eine solche Beschränkung stünde zu dem vom Unionsgesetzgeber gewählten weiten Verständnis des Begriffs «Schaden» im Widerspruch.

Zu den Regeln für die Bemessung des Schadenersatzes stellt der EuGH fest, dass Art. 82 DSGVO dahin auszulegen ist, dass es die Aufgabe der einzelnen Mitgliedstaaten ist, die Modalitäten festzulegen. Hierbei sind jedoch die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität zu beachten.

Auch im Berichtsjahr hat keine betroffene Person in Liechtenstein einen Anspruch auf Schadenersatz gegen einen Verantwortlichen oder Auftragsverarbeiter gemäss Art. 82 DSGVO geltend gemacht. Die DSS verfolgt dennoch aufmerksam die diesbezüglichen Entwicklungen im EWR und vor allem die Rechtsprechung des EuGH. Allerdings wenden sich immer wieder betroffene Personen an die DSS, um sich zu erkundigen, unter welchen Voraussetzungen sie Schadenersatz geltend machen können. Mangels nationaler Rechtsprechung zu dieser Frage verweist die DSS regelmässig auf die Rechtsprechung des EuGH.

EuGH, 4. Mai 2023, C-60/22: Bundesrepublik Deutschland (Rechte der Betroffenen)

Der EuGH hatte die Frage zu entscheiden, ob Art. 17 Abs. 1 Bst. d und Art. 18 Abs. 1 Bst. b DSGVO dahin auszulegen sind, dass der Verstoss eines Verantwortlichen gegen die Pflichten aus den Art. 26 und 30 DSGVO über den Abschluss einer Vereinbarung zur Festlegung der gemeinsamen Verantwortung für die Verarbeitung bzw. das Führen eines Verzeichnisses von Verarbeitungstätigkeiten eine unrechtmässige Verarbeitung darstellt, die der betroffenen Person ein Recht auf Löschung oder auf Einschränkung der Verarbeitung verleiht, weil ein solcher Verstoss bedeutet, dass der Verantwortliche gegen den Grundsatz der «Rechenschaftspflicht» des Art. 5 Abs. 2 DSGVO verstösst. Der EuGH verneint diese Frage.

Weiter hält der EuGH fest, dass das Unionsrecht dahin auszulegen ist, dass dann, wenn ein für die Verarbeitung personenbezogener Daten Verantwortlicher gegen seine Pflichten aus den Art. 26 oder 30 DSGVO verstossen hat, die Einwilligung der betroffenen Person keine Voraussetzung dafür darstellt, dass die Berücksichtigung dieser Daten durch ein nationales Gericht rechtmässig ist.

Die DSS berief sich in mehreren Beschwerdefällen auf diese Entscheidung, indem sie daraus ableitete, dass ein Beschwerdeführer im Rahmen einer Beschwerde gemäss Art. 77 DSGVO kein subjektives Recht auf Erstellung eines Verarbeitungsverzeichnisses oder den Abschluss eines Vertrages zur gemeinsamen Datenverarbeitung geltend machen kann. Es steht hingegen der DSS frei, in einem Beschwerdeverfahren diese Punkte amtswegig aufzugreifen und zu beurteilen.

EuGH, 22. Juni 2023, C-579/21: Pankki S (Auskunftsrecht)

Der EuGH stellt zunächst fest, dass die DSGVO, die seit dem 25. Mai 2018 gilt, auf ein nach diesem Datum vorgebrachtes Auskunftsersuchen nach Art. 15 DSGVO anwendbar ist, auch wenn die dieses Ersuchen betreffenden Verarbeitungsvorgänge vor dem Inkrafttreten der DSGVO ausgeführt wurden.

Sodann stellt der EuGH fest, dass Art. 15 Abs. 1 DSGVO dahin auszulegen ist, dass Informationen, die Abfragen personenbezogener Daten einer Person betreffen und die sich auf den Zeitpunkt und die Zwecke dieser Vorgänge beziehen, Informationen darstellen, welche die genannte Person nach dieser Bestimmung von dem Verantwortlichen verlangen darf. Dagegen sieht diese Bestimmung kein solches Recht in Bezug auf Informationen über die Identität der Arbeitnehmer dieses Verantwortlichen vor, die diese Vorgänge unter seiner Aufsicht und im Einklang mit seinen Weisungen ausgeführt haben, ausser wenn diese Informationen unerlässlich sind, um der betroffenen Person es zu ermöglichen, die ihr durch diese Verordnung verliehenen Rechte wirksam wahrzunehmen, und vorausgesetzt, dass die Rechte und Freiheiten dieser Arbeitnehmer berücksichtigt werden.

Diese Entscheidung des EuGH bestätigt die Entscheidung der DSS, dass ein Auskunftsersuchen gemäss Art. 15 DSGVO nicht das Recht mitumfasst, unter der Kategorie «Empfänger» die Offenlegung der Namen der Mitarbeitenden eines Verantwortlichen zu verlangen. Mitarbeitende sind insoweit nicht als Empfänger zu qualifizieren, als sie unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten. Lediglich in dem Falle, dass sie die Daten eigenmächtig und ausserhalb der Anweisungen der verantwortlichen Stelle verarbeiten, müsste die Rechtslage anders bewertet werden.

EuGH, 26. Oktober 2023, C-307/22: FT (Kopie der Patientenakte)

Ein Patient verlangte von seiner Zahnärztin eine unentgeltliche Kopie seiner Patientenakte, um gegen sie Haftungsansprüche wegen Fehlern geltend zu machen, die ihr bei der zahnärztlichen Behandlung unterlaufen sein sollen.

In seinem Urteil hat der EuGH entschieden, dass die erste Auskunft aus der Patientenakte nach Art. 12 Abs. 5 DSGVO sowie Art. 15 Abs. 1 und 3 DSGVO kostenlos zu sein hat und dass dies auch gelte, wenn der betreffende Antrag mit einem anderen als den in Satz 1 des 63. Erwägungsgrundes der DSGVO genannten Zwecken begründet wird. Der Patient ist nicht verpflichtet, seinen Antrag zu begründen. Selbst mit Blick auf den Schutz der wirtschaftlichen Interessen der Behandelnden dürfen die nationalen Regelungen dem Patienten nicht die Kosten einer ersten Kopie seiner Patientenakte auferlegen.

Des Weiteren hat der Patient das Recht, eine vollständige Kopie der Dokumente zu erhalten, die sich in seiner Patientenakte befinden, wenn dies zum Verständnis der in diesen Dokumenten enthaltenen personenbezogenen Daten erforderlich ist. Dies schliesst Daten aus der Patientenakte ein, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten.

Hier bestätigte der EuGH erneut den Grundsatz, dass eine verantwortliche Stelle Auskunft gemäss Art. 15 DSGVO zu erteilen hat, selbst wenn sie die Vermutung hegt, dass das Auskunftsrecht aus datenschutzfremden Gründen erfolgt. Wie bereits oben zu C-487/21 ausgeführt, kann ein Verantwortlicher gemäss DSS erst im Rahmen des Rechts auf Kopie die Erforderlichkeit der Kopie für die Ausübung der Betroffenenrechte prüfen.

EuGH, 5. Dezember 2023, C-683/21 und C-807/21: Nacionalinis visuomenės sveikatos centras und Deutsche Wohnen (Geldbussen, gemeinsame Verantwortlichkeit)

Der EuGH hat entschieden, dass gegen einen für die Datenverarbeitung Verantwortlichen nur dann eine Geldbusse wegen Verstosses gegen die DSGVO verhängt werden kann, wenn der Verstoss schuldhaft – also vorsätzlich oder fahrlässig – begangen wurde.

Handelt es sich bei dem Verantwortlichen um eine juristische Person, haftet diese nicht nur für Verstösse ihrer Vertreter, Leitungspersonen oder Geschäftsführer, sondern auch für Verstösse, die von jeder sonstigen Person begangen werden, die im Rahmen ihrer unternehmerischen Tätigkeit in ihrem Namen handelt. Ein Verstoss muss dabei keiner bestimmten natürlichen Person zugeordnet werden können. Ausserdem kann gegen einen Verantwortlichen eine Geldbusse auch für Verarbeitungsvorgänge verhängt werden, die von einem Auftragsverarbeiter durchgeführt wurden, sofern diese Vorgänge dem Verantwortlichen zugerechnet werden können.

Zur gemeinsamen Verantwortlichkeit von zwei oder mehr Einrichtungen führt der EuGH aus, dass

sich diese allein daraus ergibt, dass die Einrichtungen an der Entscheidung über die Zwecke und Mittel der Verarbeitung mitgewirkt haben. Die Einstufung als «gemeinsam Verantwortliche» setzt keine förmliche Vereinbarung zwischen den betreffenden Einrichtungen voraus.

Schliesslich muss sich die Aufsichtsbehörde bei der Bemessung der Geldbusse, wenn der Adressat ein Unternehmen ist oder zu einem Unternehmen gehört, auf den wettbewerbsrechtlichen Begriff «Unternehmen» stützen. Der Höchstbetrag der Geldbusse ist auf der Grundlage eines Prozentsatzes des gesamten Jahresumsatzes zu berechnen, den das betreffende Unternehmen als Ganzes im vorangegangenen Geschäftsjahr weltweit erzielt hat.

In einem Beschwerdefall stellte die DSS fest, dass für eine Anmeldung zu einer Veranstaltung im diesbezüglichen digitalen Anmeldeformular automatisch gewisse Daten aus einer zuvor erfolgten Anmeldung auf einer verbundenen Internetseite übernommen wurden. Die verantwortliche Stelle lehnte eine gemeinsame Verantwortung ab. Die DSS erkannte amtswegig aufgrund der tatsächlichen Verhältnisse eine solche gemeinsame Verantwortung an und wies die verantwortliche Stelle an, die Informationen gemäss Art. 13 DSGVO entsprechend anzupassen, sodass die Ansprechpersonen für die Ausübung der Betroffenenrechte transparent kommuniziert 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. Stellungnahme zu Vorlagen und Erlassen

Die DSS begutachtete im Berichtsjahr insgesamt 39 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 (VNB) der Regierung betreffend die Abänderung der Verfassung und die Schaffung eines Gesetzes über die staatlich anerkannten Religionsgemeinschaften (Religionsgemeinschaftengesetz; RelGG)** sowie die Abänderung weiterer Gesetze traf die DSS folgende Feststellungen:

Art. 24 RelGG bestimmt in Abs. 1, dass verschiedene öffentliche Stellen in ihren Registern Daten über die Religionszugehörigkeit erfassen. Abs. 2 ergänzt, dass im Zuge dieser Erfassung auch die Einwilligung der betroffenen Personen eingeholt werden soll, die es den öffentlichen Stellen erlaubt, die Daten an die entsprechende Religionsgemeinschaft weiterzugeben. Aus Sicht der DSS kann folglich Art. 24 RelGG als nationales Gesetz im Sinne des Art. 9 Abs. 2 Bst. g DSGVO qualifiziert werden. Dies bedingt allerdings, dass Art. 24 RelGG die Kriterien erfüllt, welche Art. 9 Abs. 2 Bst. g DSGVO vorsieht. Das heisst, Art. 24 RelGG sollte Ausführungen enthalten, die festlegen, dass die Datenverarbeitung in einem «angemessenen Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Massnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht und aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist». Insbesondere ist es aus Sicht der DSS unklar, warum die in Abs. 1 geregelte Datenverarbeitung, sprich die Aufnahme in die Register, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. Zudem stellt sich in Bezug auf Abs. 1 die Frage nach dem Zweck. Selbst wenn ein Zweck eventuell darin bestehen könnte, dass es, wie in Abs. 2 ausgeführt, um die Einholung der Einwilligung und Weiterleitung an die Religionsgemeinschaften geht, ist fraglich, wozu die umfassende, von der Einwilligungseinholung unabhängige Erhebung und Aufnahme der Daten in eigenen Registern erfolgt. Ebenso ist nicht eindeutig klar, ob die Weitergabe der Daten tatsächlich als öffentliche Aufgabe zu sehen ist, die im erheblichen öffentlichen Interesse liegt.

Dieselben Fragen stellen sich für die DSS auch bei der Anwendung von Art. 24 Datenschutzgesetz (DSG). Art. 24 Abs. 2 DSG regelt konkret die «Übermittlung personenbezogener Daten durch öffentliche Stellen an nicht-öffentliche Stellen» und Abs. 3 nimmt Bezug auf die Übermittlung von Daten im Sinne des Art. 9 DSGVO. Auf den konkreten Fall bezogen, verlangt Art. 24 Abs. 3 DSG das Vorliegen eines Ausnahmetatbestands gemäss Art. 9 Abs. 2 DSGVO. Folglich ist auch auf diesem Weg wieder zu prüfen, ob die Vorgaben des Art. 9 Abs. 2 Bst. g DSGVO erfüllt sind. Die Prüfung kommt zu dem oben bereits aufgezeigten Ergebnis, nämlich die Frage nach dem erheblichen öffentlichen Interesse und dem konkreten Zweck, vor allem der Erfassung in den eigenen Registern der erfassenden Stellen.

Ergänzend erwähnte die DSS noch Erwägungsgrund 55 der DSGVO, welcher Folgendes vorsieht: «Auch die Verarbeitung personenbezogener Daten durch staatliche Stellen zu verfassungsrechtlich oder völkerrechtlich verankerten Zielen von staatlich anerkannten Religionsgemeinschaften erfolgt aus Gründen des öffentlichen Interesses.» Es geht aus dem vorliegenden Gesetzesentwurf allerdings nicht hervor, dass die Datenerhebung in Art. 24 RelGG tatsächlich verfassungsrechtlich oder völkerrechtlich verankerten Zielen dient. Die anonymisierte Weitergabe der Anzahl von Angehörigen einer bestimmten Religionsgemeinschaft würde etwa für die Finanzierung der Gemeinschaften ausreichen.

In Bezug auf Art. 6 RelGG ist die vorgeschlagene Lösung zwar datenschutzkonform, da mit einer Einwilligung die Weitergabe der Daten an die Religionsgemeinschaften gemäss Art. 9 Abs. 2 Bst. a DSGVO zulässig ist. Es ist allerdings unüblich, dies gesetzlich zu verankern, da eine Datenverarbeitung auf Grundlage einer Einwilligung unabhängig von einem Gesetz jederzeit unter Einhaltung der einschlägigen Voraussetzungen gegeben werden kann. Es ist zudem auch nicht ersichtlich, warum die Weitergabe der personenbezogenen Daten dazu dienen soll, dass die Religionsangehörigen ihr Grundrecht auf Religionsfreiheit möglichst weitgehend ausleben können.

Abschliessend wies die DSS darauf hin, dass die Begriffe «Personendaten» und «bearbeiten» an die Da-

tenschutzbestimmungen angepasst und mit den Fachbegriffen «personenbezogene Daten» und «verarbeiten» ersetzt werden sollten. Ebenso sollte durchgängig der Begriff «Einwilligung» und «betroffene Person» verwendet werden, wenn diese Begriffe in einem datenschutzrechtlichen Kontext zur Anwendung gelangen.

In Bezug auf den **Vernehmlassungsbericht (VNB) der Regierung betreffend die Totalrevision des Archivgesetzes** vom 23. Oktober 1997 brachte die DSS eine umfangreiche Stellungnahme ein und wies dabei neben einigen begrifflichen Korrekturvorschlägen auf die folgenden kritischen Punkte hin:

Art. 6 Abs. 1 Archivgesetz findet seinem Wortlaut nach Anwendung auf sämtliche Unterlagen, die bei den in Art. 3 Bst. e genannten Stellen anfallen und die nicht mehr benötigt werden. Die Endentscheidung über die Archivwürdigkeit trifft das Landesarchiv. Aus Sicht des Datenschutzes wäre es sehr ratsam, zumindest auf Verordnungsweg eine Liste mit Unterlagen zu erstellen, auf welche die Archivwürdigkeit definitiv nicht zutrifft und die damit nicht der Endentscheidung des Landesarchivs unterfallen. Ein Beispiel sind etwa Bewerbungsunterlagen von Personen, die eine Absage erhalten. Aus Sicht der Datenschutzgesetzgebung sind diese Daten nach 4-5 Monaten definitiv zu löschen. Eine Archivwürdigkeit kann und sollte daher von vornherein für solche Fälle ausgeschlossen werden.

Art. 6 Abs. 1 Archivgesetz bestimmt: «1) Unterlagen, die bei den im Art. 3 Bst. e genannten Stellen anfallen und die nicht mehr benötigt werden, sind regelmässig nach Ablauf der geltenden gesetzlichen Aufbewahrungsfrist bzw. der Aufbewahrungsfrist gemäss geltendem Aktenplan […] aufzubewahren.» In Art. 7 Abs. 2 und Art. 8 Abs. 2 werden die «gesetzlichen Aufbewahrungsfristen» hingegen nicht mehr genannt bzw. durch den engeren Begriff der Fristen in Gemeindeordnungen bzw. in Reglementen ersetzt. Dies ist insofern nicht korrekt, als sämtliche Institutionen gesetzlichen Aufbewahrungspflichten unterliegen, die über die Gemeindeordnung oder Reglemente hinausgehen. Die DSS regt daher eine Vereinheitlichung der Formulierung an.

Art. 9 Abs. 3 Archivgesetz sieht vor, dass für den Katastrophenfall Kopien des Archivguts im Ausland aufbewahrt werden. Die DSS empfiehlt, zumindest in den Erläuterungen darauf hinzuweisen, dass dies für den Fall, dass das Archivgut personenbezogene Daten beinhaltet, nur unter der Einhaltung des Kapitel V DSGVO stattfinden kann.

In Bezug auf Art. 10 Abs. 3 Archivgesetz stellt sich die Frage, aus welchem Grund der Gesetzesartikel sowohl auf Art. 9 und Art. 10 DSGVO Bezug nimmt, während die Erläuterungen lediglich Daten im Sinne des Art. 9 DSGVO erwähnen. Inhaltlich ist für die DSS zudem nicht ersichtlich, warum sich diese verlängerte Schutzfrist nur auf besondere Kategorien personenbezogener Daten bezieht und nicht sämtliche personenbezogenen Daten umfasst. Diese Trennung erscheint nicht nur aus datenschutzrechtlicher Perspektive fragwürdig, sondern auch aus praktischen Überlegungen. Es würde nämlich bedeuten, dass man die Unterlagen jeweils im Vorfeld «klassifizieren» müsste. Zudem zeigt die jüngere Rechtsprechung des EuGH, dass die Grenzen zwischen «normalen» und «sensiblen» Daten fliessend sind und vor allem vom EuGH selbst jederzeit verschoben werden können. Die DSS empfiehlt darüber hinaus eine Bestimmung aufzunehmen, welche eine Unterscheidung macht zwischen personenbezogenen Daten betroffener Personen und den jeweiligen Personen, die für eine öffentliche Stelle handeln. Besonderer Schutz sollte vor allem der ersten Kategorie betroffener Personen zukommen.

Art. 12 Archivgesetz befasst sich mit dem Recht auf Auskunft und Berichtigung und passt diese Rechte auf den Fall der Archivierung an. Art. 12 Abs. 1 vermittelt den Eindruck, dass das hier festgelegte Auskunftsrecht nur dann zum Tragen kommt, soweit nicht ohnehin ein gesetzliches Auskunftsrecht besteht. Korrekterweise handelt es sich im vorliegenden Fall nicht um ein zusätzliches Auskunftsrecht, sondern um eine Einschränkung des allgemeinen Auskunftsrechts des Art. 15 DSGVO, in Bezug auf welches Mitgliedstaaten gemäss Art. 23 DSGVO gewisse Einschränkungen vornehmen dürfen. In Liechtenstein wurde von dieser Möglichkeit bereits mit Art. 29 Abs. 4 DSG Gebrauch gemacht.

Art. 29 Abs. 4 DSG sieht für den Fall von Archiven im öffentlichen Interesse folgende Einschränkung vor:

«4) Das Recht auf Auskunft der betroffenen Person nach Art. 15 der Verordnung (EU) 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.»

Dieser Absatz 4 ist zwar dem Art. 12 Abs. 1 des neuen Archivgesetzes recht ähnlich, im Detail ergeben sich aber Widersprüchlichkeiten, vor allem im Hinblick auf die Bst. b und c in Art. 12 des neuen Archivgesetzes. Die DSS empfiehlt daher eine Präzisierung mit dem Ziel der Vereinheitlichung des Art. 29 Abs. 4 DSG und des Art. 12 Abs. 1 neues Archivgesetz.

Art. 12 Abs. 3 Archivgesetz sieht zudem eine weitere Einschränkung des Auskunftsrechts vor, nämlich aus den drei in den Bst. a-c genannten Gründen. Die Bst. b und c entsprechen dem Art. 23 DSGVO, bei Bst. a hingegen ist nicht ganz klar, welcher Ausnahmemög-

lichkeit des Art. 23 DSGVO dies entspricht. Die DSS empfiehlt eine diesbezügliche Prüfung.

In Bezug auf das Recht auf Berichtigung und mögliche Einschränkungen heisst es in Art. 29 Abs. 5 DSG:

«5) Das Recht auf Berichtigung der betroffenen Person nach Art. 16 der Verordnung (EU) 2016/679 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.»

Demgegenüber ist die Formulierung in Art. 12 Abs. 4 neues Archivgesetz um einiges strenger bzw. ist für den Rechtsanwender nicht ganz klar, ob es sich vielleicht um zwei unterschiedliche Regelungen handelt, da das DSG von «Richtigkeit der personenbezogenen Daten» spricht und Art. 12 Abs. 4 Archivgesetz von «falschen Tatsachenbehauptungen». Auch hier empfiehlt die DSS, den Zusammenhang zwischen den beiden Gesetzesbestimmungen zu überprüfen und zu präzisieren.

Schliesslich ist darauf hinzuweisen, dass Art. 29 Abs. 6 DSG festhält, dass «Die in Art. 18 Abs. 1 Bst. a, b und d, Art. 20 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte nicht bestehen, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.» Die DSS empfiehlt, diesen Ausschluss der weiteren Betroffenenrechte zumindest mit Verweis in das neue Archivgesetz aufzunehmen.

«Die bereits in den Vorjahren praktizierte intensive Zusammenarbeit zwischen Technik und Recht war auch im Berichtsjahr unabdingbar für die Tätigkeiten der DSS.»

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 an sie gestellten Anforderungen und unter Einsatz eines bestehenden Personals von 700 Stellenprozenten ihre Aufgaben im Berichtsjahr bewältigen, allerdings bisweilen mit einer gewissen zeitlichen Verzögerung. Bedingt war dies neben den stark steigenden Anforderungen im Berichtsjahr dadurch, dass das Team aufgrund einer unbesetzten Juristenstelle über einen Zeitraum von einem halben Jahr mit einer erheblichen Arbeitsbelastung konfrontiert war. Erst im Oktober konnte die vakante Juristenstelle wiederbesetzt werden. Im September verstärkte zudem eine Rechtspraktikantin das Team mit 100 Stellenprozent sowie zwischen Oktober und Dezember mit 20 Stellenprozenten.

Die bereits in den Vorjahren praktizierte intensive Zusammenarbeit zwischen Technik und Recht war auch im Berichtsjahr unabdingbar für die meisten Tätigkeiten der DSS. Insbesondere die Frage nach der Zulässigkeit von Webanalyse-Tools etc. war beispielsweise fast täglich präsent und die Beurteilung von neuen Technologien verlangte nach vertieftem technischem Verständnis.

4.2 Personal Schengen-Evaluation

Die gesetzlichen Grundlagen diverser EU-Informationssysteme im Schengen-Raum sehen vor, dass diese alle vier Jahre einer datenschutzrechtlichen Kontrolle unterzogen werden müssen. Aufgrund der Mitgliedschaft Liechtensteins im Schengen-Raum entsandte die DSS im Berichtsjahr in einem Fall einen Experten zwecks Evaluierung eines anderen Schengen-Staates.

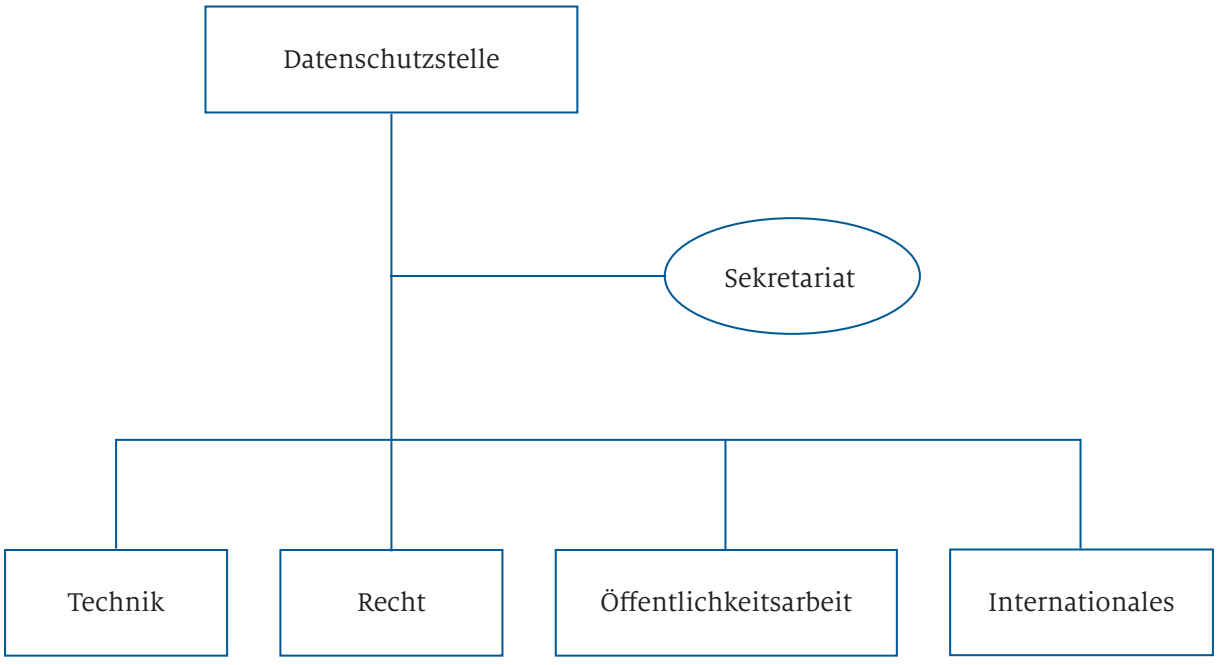


Abbildung 3: Organigramm Datenschutzstelle

«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.

5.1.1 Amtswegige Überprüfungen bei Unternehmen

Auf Grund der knappen personellen Ressourcen entschied die DSS, im Berichtsjahr auf amtswegige Überprüfungen bei Unternehmen zu verzichten. Die im Vorjahr begonnenen amtswegigen Untersuchungen konnten im Berichtsjahr fast vollständig erfolgreich abgeschlossen werden. Zudem wurden drei zusätzliche Untersuchungen bei verschiedenen Organisationen eingeleitet, nachdem Zweifel an deren Datenschutzkonformität im Rahmen von Anfragen an die DSS aufgekommen waren.

Nachdem die Erkenntnisse aus diesen amtswegigen Verfahren doch einen beträchtlichen Wert für die DSS haben, indem sie einen guten Überblick über den Umsetzungsstand der DSGVO in Liechtenstein geben, plant die DSS, spätestens im Herbst 2024 zumindest wieder einzelne amtswegige Überprüfungen zu lancieren.

5.1.2 Amtswegige Überprüfung des Bedrohungsmanagements der Landespolizei

Mit Bericht und Antrag 128/2016 wurde das Polizeigesetz ergänzt und nach der Rezeptionsvorlage des Kantons Solothurn ein Bedrohungsmanagement in Liechtenstein eingeführt. Die dafür aufgebaute Fachstelle der Landespolizei ist seit Januar 2020 voll funktionsfähig. Im letzten Tätigkeitsbericht hatte die DSS bereits über die Eröffnung und Durchführung einer Überprüfung des Bedrohungsmanagements informiert. Im Berichtsjahr konnte die Kontrolle abgeschlossen werden. Die umfassende Überprüfung ergab, dass die Abläufe und Datenverarbeitungen datenschutzkonform ausgestaltet sind und im zuständigen Team eine Datenschutzsensibilität besteht. Einzige Beanstandung war die Nichtdurchführung einer Datenschutz-Folgenabschätzung vorgängig zur Einführung des Bedrohungsmanagements.

5.1.3 Aufsicht über Videoüberwachungsanlagen

Im Bereich der Videoüberwachungen zeigte sich auch im Berichtsjahr erneut, dass eine klare Trennung zwischen Beratung und Beschwerde schwieriger ist als in Fällen von anderen Datenverarbeitungen. Die Grenze ist oft fliessend, da die betroffenen Personen selbst nicht immer sicher sind, ob sie wirklich eine formelle Beschwerde einbringen wollen oder nicht. Die DSS akzeptiert daher auch «informelle» Beschwerden, vor allem wenn es sich um Videokameras im nachbarschaftlichen Umfeld handelt. Dies ermöglicht es der DSS, im Rahmen eines beratenden Ansatzes auf eine datenschutzkonforme Lösung hinzuwirken. Erst wenn dies zu keiner zufriedenstellenden Lösung führt, geht das Verfahren in eine formelle Prüfung über, welche mit einer Verfügung ihren Abschluss findet.

In allen Fällen des Berichtsjahrs fand daher in einem ersten Schritt eine Vor-Ort-Begehung und eine Besprechung mit den Betroffenen wie auch den Verantwortlichen statt. War die Kontaktaufnahme mit den Verantwortlichen auf diese Weise nicht möglich, nahm die DSS telefonisch oder mittels Behördenbrief Kontakt zu ihnen auf. Alle Videoüberwachungen konnten so datenschutzrechtlich konform umgesetzt werden.

Insgesamt konnte die DSS feststellen, dass Videoüberwachungen, die in nachbarschaftlichen Verhältnissen zum Einsatz kommen, auf unterschiedliche Weise Anlass zu Konflikten geben können. Zum einen ist es direkt die Videoüberwachung, die bei Nachbarn Grund zur Sorge auslöst. Zum anderen handelt es sich

um Nachbarschaftsstreitigkeiten, die oft Jahre zurückgehen, und der Streitpunkt bezüglich einer Videoüberwachung ist dann nur mehr der «Tropfen, der das Fass zum Überlaufen bringt». Wie auch immer der konkrete Kontext ausgestaltet ist, nimmt die DSS diese Anliegen sehr ernst und beurteilt die Sachlage aus objektiver datenschutzrechtlicher Sicht. Zusammenfassend kann festgehalten werden, dass die Überwachung von Privatgrundstücken grundsätzlich zulässig ist, solange nicht mehrere Parteien Nutzniesser dieser Grundstücke sind. Aber selbst datenschutzrechtlich zulässige Videoüberwachungen können zu Konflikten führen, da je nach eingesetzter Kamera nicht immer gut erkennbar ist, ob eine Kamera überhaupt in Betrieb ist bzw. welcher Bereich konkret überwacht wird. Schliesslich kann selbst in Fällen, in denen gar keine (rechtswidrige) Datenverarbeitung vorliegt, ein subjektiv empfundener Überwachungsdruck entstehen. Dieser Umstand fällt grundsätzlich in den Bereich des PGR und die DSS ist hierfür nicht zuständig. Sie informiert jedoch im Rahmen ihrer Beratung regelmässig auch über rechtliche Möglichkeiten in Zusammenhang mit einem potentiellen Überwachungsdruck.

5.1.4 Schengen-Evaluationen

Für die regelmässige datenschutzrechtliche Evaluation der diversen europäischen Informationssysteme in den Mitgliedstaaten wurde bisher jeweils ein Expertenteam bestehend aus Mitarbeitenden der EU-Kommission wie auch EU/EWR-Aufsichtsbehörden zusammengestellt, welches eine Vor-Ort-Kontrolle durchführt. Der Prozess sowie die Organisation der Durchführung dieser Evaluationen wurde kürzlich überarbeitet und angepasst und kam im Berichtsjahr zum ersten Mal zum Einsatz. Neu werden von den Evaluationsteams nicht mehr mehrere eigenständige Berichte (z.B. in den Bereichen Datenschutz, Grenzen, Polizeikooperation etc.) erstellt, sondern es gibt einen gemeinsamen Bericht, bei dem die Datenschutzevaluation lediglich einen Bestandteil darstellt. Dies soll unter anderem den Arbeitsaufwand für die Vor-Ort-Kontrollen minimieren. Weiters werden nur noch Elemente in den Bericht aufgenommen, welche entweder eine «Best Practice» darstellen oder Nachbesserungen erfordern. So entfällt der grosse, lediglich deskriptive Teil des Abschlussberichts. Positiv hervorzuheben ist zudem die Tatsache, dass neu Experten aus operativen Behörden, wie SIRENE-Büros, Polizei und Visavergabestellen die Datenschutzevaluationsteams ergänzen. Diese bringen einen anderen Blickwinkel mit und ein tiefergehendes Fachwissen, gerade im Bereich der Prozesse und Abläufe in den jeweiligen Bereichen. So können konkretere Fragen gestellt werden und die anderen Evaluationsteammitglieder können von dieser Expertise profitieren. Im Rahmen dieser Schengen-Evaluationen entsandte die DSS im Oktober einen Juristen nach Lettland.

Des Weiteren fand im Berichtsjahr ein online-Training für Schengen-Experten statt. Nach einer allgemeinen Einführung wurde im Rahmen einer fiktiven Kontrolle einer EWR-Datenschutzaufsichtsbehörde das Gelernte angewandt und weiter vertieft. Das Training richtete sich insbesondere an neue Experten ohne Erfahrung in Schengen-Evaluationen. Auch von Seiten der DSS hat ein IT-Experte daran teilgenommen.

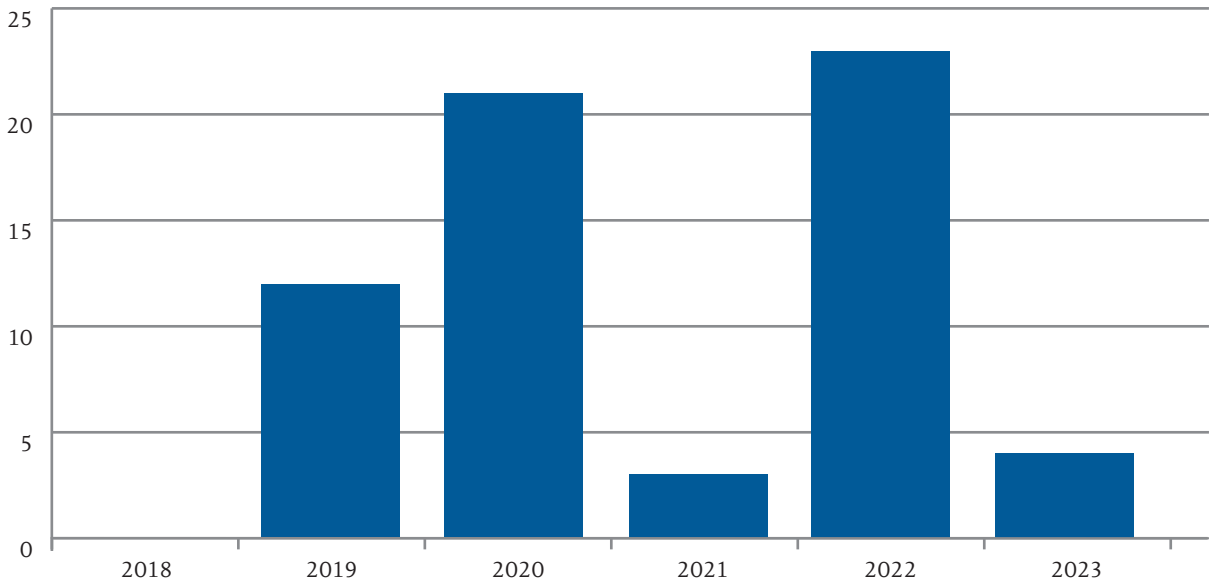


Abbildung 4: Anzahl der Datenschutzüberprüfungen pro Jahr (ohne Videoüberwachungen)

5.2 Beschwerden

Betroffene Personen haben nach Art. 77 DSGVO das Recht, sich bei der Aufsichtsbehörde zu beschweren, wenn sie der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten nicht rechtmässig erfolgt. Dazu bietet die DSS – wie in Erwägungsgrund 141 der DSGVO empfohlen – auf ihrer Internetseite in der Rubrik «Services» ein elektronisches Beschwerdeformular an.

Im Berichtsjahr erhielt die DSS insgesamt 44 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.

Zusätzlich erhielt die DSS im Rahmen der Zusammenarbeit mit den anderen Aufsichtsbehörden im EU/EWR-Raum unter Art. 56 ff. DSGVO im Berichtsjahr eine weitere Beschwerde einer Person aus einem anderen Mitgliedstaat, die sich gegen ein liechtensteinisches Unternehmen richtete. Zudem leitete die DSS eine Beschwerde einer Person aus Liechtenstein an eine andere europäische Datenschutzbehörde weiter. Damit lag die Anzahl der Beschwerden gemäss Art. 77 DSGVO bei der DSS rund 2% über der Anzahl des Vorjahres.

Inhaltlich konzentrierten sich die Beschwerdeverfahren erneut auf die Rechte auf Information, Auskunft, Löschung und Widerspruch sowie die Frage der Rechtmässigkeit der Datenverarbeitung gemäss Art. 6 Abs. 1 oder Art. 9 Abs. 2 DSGVO.

Die DSS machte von ihren Befugnissen unter Art. 58 Abs. 2 DSGVO weitreichend Gebrauch und sprach Verwarnungen, Anweisungen, Beschränkungen und Verbote aus. Lediglich in einem Fall wurde eine Geldbusse in Höhe von CHF 500 verhängt, welche mittlerweile auch rechtskräftig ist. Damit ist die DSS nach wie vor im Vergleich zu den anderen europäischen Behörden eher die Ausnahme, denn die Geldbussen nehmen im EU/EWR-Raum beständig zu und werden gerade in Fällen von beharrlichen und weitreichenden Datenschutzverletzungen oft als das einzige tatsächlich abschreckende Mittel gesehen.

Die sehr strenge Auslegung der Beschwerdekommission für Verwaltungsangelegenheiten (VBK) des Art. 40 Abs. 6 DSG lässt der DSS allerdings wenig Spielraum, da die VBK trotz des darin zweifach genannten und nicht abschliessenden Kriteriums «insbesondere» im Jahr 2020 feststellte, dass in jedem Fall vor Verhängung einer Geldbusse eine Verwarnung im Sinne des Art. 58 Abs. 2 Bst. b DSGVO zu erfolgen hat. Selbst im Fall eines schwerwiegenden und weitreichenden Verstosses könnte damit als strengste Sanktion lediglich eine Verwarnung, entsprechende Anweisung oder weitere Massnahme im Sinne des Art. 58 Abs. 2 DSGVO erfolgen. Dies widerspricht aus Sicht der DSS eindeutig dem Grundgedanken und der risikobasierten Ausrichtung der DSGVO, wonach auch eine Sanktion einer Aufsichtsbehörde immer an der Schwere des Verstosses bzw. des Risikos und der Konsequenzen für die betroffenen Personen auszurichten ist. So muss eine jede der Sanktionen gemäss Art. 83 und 84 DSGVO «wirksam, verhältnismässig und abschre-

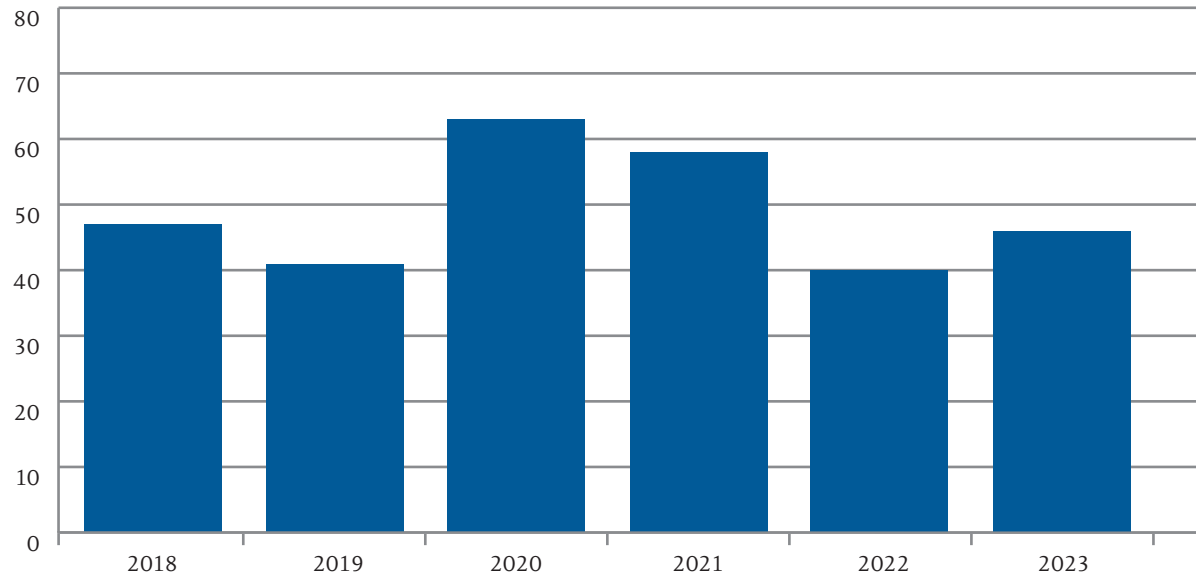


Abbildung 5: Anzahl der Beschwerden pro Jahr

ckend» sein. Bei schwerwiegenden und weitreichenden Verstössen wäre diese Vorschrift aber mit einem generellen Verzicht auf Geldbussen bei erstmaligen Verstössen kaum einzuhalten.

Nicht in jedem Beschwerde-Fall bildete eine Verfügung den Abschluss des Verfahrens. Stattdessen konnte in einigen Fällen mit der datenverarbeitenden 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 zahlreiche langwierige und aufwändige Verfahren verhindert werden.

5.2.1 Ausgewählte Verfügungen der DSS im Berichtsjahr

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

Beschwerde betreffend Datenoffenlegung

Seit 2021 beschäftigte sich die DSS mit einem Konflikt zwischen zwei Privatpersonen, in denen sich mehrfache datenschutzrechtliche Fragen stellten. Während einige der Fragen durch Beratungen seitens der DSS beantwortet werden konnten, kam es in Bezug auf eine Datenoffenlegung zu einem Beschwerdeverfahren. In diesem Fall wurde von einer Privatperson eine Fotoaufnahme eines Autos (mit erkennbarem Kennzeichen) des Beschwerdeführers wie auch Akten, die aus einem Strafverfahren stammen, an eine dritte Person weitergegeben. Die DSS kam zum Schluss, dass die Weitergabe des Fotos gestützt auf Art. 6 Abs. 1 Bst. f DSGVO datenschutzrechtlich zulässig war, da dafür auch das berechtigte Interesse der dritten Person ausreichend sein kann, wenn dieses die Interessen der betroffenen Person überwiegt. In Bezug auf die Akten aus einem Strafverfahren kam die DSS zum Schluss, dass eine Weitergabe datenschutzrechtlich unzulässig war. Es war zunächst festzustellen, dass zwischen den Zwecken der Akteneinsicht in Zusammenhang mit einem bestimmten Strafverfahren und der Aktenweitergabe zur Geltendmachung von Rechten einer dritten Person (in einem anderen Verfahren) keine datenschutzrechtliche Verbindung besteht. Des Weiteren war festzuhalten, dass es sich um Daten, die im Rahmen von Ermittlungen in einem Strafverfahren erfasst wurden, handelte. Dabei handelt es sich um sensible und umfassende Daten. Art. 6 Abs. 4 DSGVO ermöglicht eine Datenweitergabe zu einem anderen Zweck als zu dem sie ursprünglich erfasst wurden nur in dem Fall, dass die Zwecke vereinbar bzw. wenn die betroffene Person mit der Datenweitergabe rechnen kann. Da diese Vorhersehbarkeit im konkreten Fall nicht gegeben war, war die Weitergabe nicht datenschutzkonform.

Beschwerde betreffend das elektronische Gesundheitsdossier (eGD)

Im Februar 2023 brachte eine betroffene Person bei der DSS eine Beschwerde gegen das elektronische Gesundheitsdossier (eGD) ein. Die Beschwerdeführerin (Bf) brachte vor, dass am 12. Januar 2023 die Informationsbroschüre «Elektronisches Gesundheitsdossier» an alle Haushalte zugestellt und in dieser über das Recht des Widerspruchs informiert worden sei. Von diesem Recht habe die Bf Gebrauch machen wollen und festgestellt, dass dies online ohne digitale Identität (eID) nicht möglich sei. Als Alternative sei ein Formular zugestellt worden, welches jedoch eine Passkopie und die Kopie der Krankenversicherungskarte verlange. Das weitere Vorbringen betraf unter anderem Fragen nach der Zulässigkeit des gewählten Opt-out-Verfahrens an Stelle einer datenschutz-freundlicheren Opt-in-Variante, der nicht durchgängig genannten Möglichkeit der Erfassung von genetischen Daten im eGD, der Sicherheit der System-Schnittstellen und der fehlenden umfassenden Information und Aufklärung von Nutzen und Risiken.

Die DSS führte in ihrer Verfügung aus, dass die Regierung die Entscheidung getroffen hat, das eGD als eine «Aufgabe, die im öffentlichen Interesse liegt», zu qualifizieren. Art. 6 Abs. 1 Bst. e DSGVO erlaubt die Verarbeitung personenbezogener Daten, soweit dies für die Erfüllung einer solchen im öffentlichen Interesse liegenden Aufgabe erforderlich ist. Art. 6 Abs. 3 DSGVO präzisiert, dass für die Datenverarbeitung im Rahmen einer im öffentlichen Interesse liegenden Aufgabe eine nationale Rechtsgrundlage zwingend erforderlich ist. Des Weiteren werden Kriterien aufgelistet, welche die nationale Rechtsgrundlage erfüllen «kann». Für die besonderen Kategorien von personenbezogenen Daten finden Art. 9 Abs. 2 Bst. g, h und i DSGVO Anwendung, welche die Verarbeitung besonderer Kategorien von personenbezogenen Daten ebenfalls auf Grundlage eines nationalen Gesetzes zulassen. Art. 9 Abs. 2 Bst. g DSGVO verlangt dafür etwa ein «erhebliches öffentliches Interesse». Hingegen macht die DSGVO keine Vorgaben, was unter einer «im öffentlichen Interesse liegenden Aufgabe» bzw. einem «erheblichen öffentlichen Interesse» zu verstehen ist. Dies obliegt vielmehr der Beurteilung der zuständigen nationalen Entscheidungsträger und verbleibt somit in der Entscheidungshoheit der Mitgliedstaaten. Einzige Vorgabe der DSGVO ist, dass die Datenverarbeitung, die mit einer diesbezüglichen Entscheidung verbunden ist, in einem nationalen Gesetz geregelt werden muss, das «in angemessenem Verhältnis zu

dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Massnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht». Das Gesetz vom 7. Mai 2021 über das elektronische Gesundheitsdossier (EGDG) ist in Liechtenstein in einem demokratischen Prozess geschaffen worden und erhielt die Zustimmung aller Abgeordneten des Landtags. Es liegt folglich nicht in der Kompetenz der DSS, zu beurteilen, ob die genannten Entscheidungsträger korrekt gehandelt haben, indem sie das eGD als (erhebliches) öffentliches Interesse qualifiziert haben. Die Aufgabe der DSS besteht lediglich darin, zu überprüfen, ob das EGDG die Kriterien des Art. 6 Abs. 3 DSGVO bzw. des Art. 9 Abs. 2 Bst. g, h und i DSGVO erfüllt, wenngleich zu betonen ist, dass diese Kriterien zum Teil nicht zwingend sind.

Bezugnehmend auf die «Kann»-Bestimmung in Art. 6 Abs. 3 DSGVO ergab die Prüfung der DSS, dass das EDGD die genannten Kriterien erfüllt: Das EGDG spezifiziert die Art der verarbeiteten Daten (Art. 3), die betroffenen Personen (Art. 3 Abs. 1 Bst. a und b), die Offenlegung der Daten an mögliche Empfänger (Art. 5 und 12), die Speicherdauer (Art. 10) und die verwendeten Verarbeitungsvorgänge und -verfahren (Art. 5 und 7). Zudem enthält das EGDG unter anderem mit dem Widerspruchsrecht und den in Art. 9 EGDG geforderten technischen und organisatorischen Massnahmen angemessene und spezifische Massnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person. Die DSS stellt somit fest, dass das EGDG die genannten «Kann»-Kriterien des Art. 6 Abs. 3 erfüllt. Weitere Präzisierungen erfolgen in der Verordnung vom 6. Dezember 2022 über das elektronische Gesundheitsdossier (EGDV). Aus Sicht der DSGVO gilt eine Verordnung ebenso wie ein Gesetz als nationale Rechtsgrundlage und es liegt nicht im Kompetenzbereich der DSS zu beurteilen, warum gewisse Elemente betreffend eGD in der Verordnung und nicht dem Gesetz behandelt werden.

Art. 6 Abs. 3 DSGVO enthält zudem das zwingende Erfordernis, dass die Rechtsgrundlage den Zweck festlegen muss. Dies ist in Art. 1 EGDG erfüllt. Das nationale Gesetz (und die damit verbundene Datenverarbeitung) muss ausserdem in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen. Auf Grund der Möglichkeit, dass betroffene Personen der Datenverarbeitung im eGD widersprechen oder im Falle einer Nutzung des eGD individuelle Entscheidungen zur Speicherung und Offenlegung ihrer Daten treffen können, ist festzustellen, dass die Datenverarbeitung in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck steht.

Die DSS stellte allerdings amtswegig fest, dass Art. 1 Abs. 3 EGDG insofern im Widerspruch zur Zweckbestimmung in Art. 1 Abs. 2 steht, als Abs. 3 auf die Rechtsgrundlagen des Art. 9 Abs. 2 Bst. g-j DSGVO verweist. Während die Bst. g, h und i mit dem Zweck des eGD übereinstimmen, ist dies in Bezug auf den Bst. j nicht der Fall. Der Zweck bzw. die öffentlichen Interessen decken keine Datenverarbeitung für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke ab. Die DSS stellte folglich amtswegig eine Rechtswidrigkeit in Bezug auf die Rechtsgrundlagen gemäss Art. 9 Abs. 2 DSGVO fest und erteilte der Beschwerdegegnerin (Bg) eine entsprechende Anweisung.

Art. 9 Abs. 3 DSGVO verlangt in Bezug auf eine Datenverarbeitung gemäss Art. 9 Abs. 2 Bst. h DSGVO, dass die Personen, welche die betreffenden Daten verarbeiten, einem Berufsgeheimnis oder einer gesetzlich geregelten Geheimhaltungspflicht unterliegen. Dies ist ebenfalls erfüllt, da Art. 38 des Staatspersonalgesetzes die Mitarbeitenden des Amts für Gesundheit sowie des Amts für Informatik verpflichtet, das Amtsgeheimnis zu wahren.

Die Feststellung der Bf, dass «der Datenschutz eine explizite Einwilligung zur Verarbeitung von personenbezogenen Daten voraussetze», ist somit nicht korrekt, da die Einwilligung nur eine der in den Art. 6 Abs. 1 und Art. 9 Abs. 2 DSGVO aufgezählten Rechtfertigungsgründe ist. Sie ist daher nicht zwingend in jedem Fall einer Datenverarbeitung einzuholen. Die Wahl des Prozedere mittels eGD als «Aufgabe im (erheblichen) öffentlichen Interesse» in Verbindung mit einem Widerspruchsrecht gemäss Art. 21 DSGVO ist eine rechtskonforme Basis für die gegenständliche Datenverarbeitung. Die Daten im eGD, einschliesslich sensibler Daten, werden somit auf «rechtmässige Weise» im Sinne des Art. 5 Abs. 1 Bst. a DSGVO iVm Art. 6 Abs. 1 Bst. e und Art. 9 Abs. 2 Bst. g, h und i DSGVO verarbeitet.

In Bezug auf die Datenkategorien der Gesundheitsdaten und genetischen Daten stellte die DSS fest, dass Art. 1 Abs. 1 EGDG bestimmt: «Dieses Gesetz regelt die Führung des elektronischen Gesundheitsdossiers und legt die Voraussetzungen für die darin verarbeiteten personenbezogenen Gesundheitsdaten und genetischen Daten fest.» Der Begriff «genetische Daten» wird in Art. 4 Ziff. 13 DSGVO sowie der Begriff «Gesundheitsdaten» in Art. 4 Ziff. 15 DSGVO definiert. Nachdem diese beiden Kategorien sensibler Daten Teil der Gesundheitshistorie eines Menschen sein können, ist es folgerichtig, dass das EGDG den betroffenen Personen die Möglichkeit bietet, dass sowohl Gesundheitsdaten als auch genetische Daten im eGD verarbei-

tet werden können. Von besonderer Relevanz ist dies, wenn etwa die beiden Datentypen in einem medizinischen Befund nicht getrennt werden können. Wie von der Regierung in ihrer Stellungnahme an den Landtag zu den anlässlich der ersten Lesung betreffend die Schaffung des EGDG (BuA Nummer 2021/2) aufgeworfenen Fragen ausgeführt, steht es auch hier wieder der betroffenen Person frei, die Speicherung und Weitergabe insbesondere von genetischen Daten zu unterbinden.

Es war allerdings der Bf beizupflichten, dass der Begriff der «genetischen Daten» auch in dem an alle Haushalte versandten Flyer hätte genannt werden sollen. Die DSS empfiehlt daher der Bg, künftig durchgängig auf die parallele Nennung der beiden Begriffe zu achten und die Bevölkerung diesbezüglich umfassend zu informieren. Die DSS sieht aber diese Nachlässigkeit in Bezug auf den Flyer nicht als Verletzung einer Datenschutzbestimmung an, da ausserhalb des Flyers diese Information bezüglich der genetischen Daten umfassend vorhanden war.

In Bezug auf die Modalitäten der Ausübung des Widerspruchsrechts stellte die DSS fest, dass Art. 12 Abs. 2 DSGVO verlangt, dass der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte gemäss den Art. 15 bis 22 erleichtert. Erwägungsgrund 59 ergänzt, dass «Modalitäten festgelegt werden sollten, die einer betroffenen Person die Ausübung der Rechte, die ihr nach dieser Verordnung zustehen, erleichtern, darunter auch Mechanismen, die dafür sorgen, dass sie unentgeltlich insbesondere Zugang zu personenbezogenen Daten und deren Berichtigung oder Löschung beantragen und gegebenenfalls erhalten oder von ihrem Widerspruchsrecht Gebrauch machen kann. So sollte der Verantwortliche auch dafür sorgen, dass Anträge elektronisch gestellt werden können, insbesondere wenn die personenbezogenen Daten elektronisch verarbeitet werden.»

Das Amt für Gesundheit (AG) stellt folgende Möglichkeiten zur Geltendmachung des Widerspruchsrechts zur Verfügung:

a. über das Zugangsportal des elektronischen Gesundheitsdossiers mittels eID.
b. mittels Ausfüllens des Antragsformulars, das elektronisch auf der Webseite des AG heruntergeladen oder beim AG abgeholt oder von diesem auf Anfrage per Post oder E-Mail zugeschickt werden kann. Zusätzlich ist in diesem Falle beim Einreichen des Antrags eine Kopie des Lichtbildausweises vorzulegen.
c. durch persönliche Vorsprache beim AG unter Vorweis eines Lichtbildausweises.

Damit war von der DSS festzustellen, dass die Bg sowohl «digitale» als auch «analoge» Wege des Widerspruchs zulässt. Was den Schwierigkeitsgrad der Ausübung des Rechts auf Widerspruch betrifft, stellt die DSS fest, dass die Bg diesen im Zuge des gegenständlichen Verfahrens insofern reduziert hat, als nunmehr lediglich die Vorlage eines Identitätsausweises und nicht mehr zusätzlich auch der Krankenversicherungskarte erforderlich ist. Diese Einschränkung wird von der DSS begrüsst.

Zur Beantwortung der Frage, ob die betroffene Person auch ein Recht hat, gegen die Verarbeitung der Administrativdaten Widerspruch gemäss Art. 21 DSGVO einzulegen oder eine Löschung gemäss Art. 17 DSGVO zu verlangen, sind folgende Bestimmungen zu beachten: Art. 21 Abs. 1 DSGVO lautet: «Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen». Das EGDG erlaubt einer betroffenen Person, ohne Angabe von Gründen, der Verarbeitung der «inhaltlichen» Daten des eGD zu widersprechen. Für die Administrativdaten sieht das EGDG diese Möglichkeit nicht vor, weshalb Art. 21 Abs. 1 DSGVO zur Anwendung gelangt und die betroffene Person Gründe für den Widerspruch vorbringen muss, die sich aus ihrer «besonderen Situation» ergeben. Dieses Kriterium der «besonderen Situation» wurde von der Bf nicht vorgebracht oder näher definiert. Nachdem das Amt für Gesundheit eine gesetzliche Verpflichtung – sowohl unter dem EGDG als auch gemäss der Dokumentations- bzw. Rechenschaftspflicht gemäss Art. 5 Abs. 2 DSGVO – hat, den Widerspruch der betroffenen Person zu dokumentieren, gelangt die DSS zum Schluss, dass das AG «zwingende schutzwürdige Gründe» für die Verarbeitung der Administrativdaten gemäss Art. 21 Abs. 1 DSGVO hat und folglich die Weigerung, das Widerspruchsrecht der betroffenen Person anzuerkennen, rechtmässig erfolgt.

Zur Frage der Sicherheit der «Systemschnittstellen» zur eHealth-Plattform war von der DSS festzustellen, dass die technischen und organisatorischen Massnahmen, die von der Verantwortlichen und dem Auftragsverarbeiter ergriffen wurden, auch für eine adäquate Sicherheit der Schnittstellen im Sinne des Art. 32 DSGVO sorgen. Ebenso ist festzustellen, dass der Gesetzgeber mit dem Art. 9 EGDV die genannten Bestimmungen der DSGVO wiederholt bzw. konkretisiert und die EGD-Gesundheitsdienstleister auf ihre Verpflichtungen bezüglich technischer und organisatorischer Massnahmen hinweist: «2) Wird der Zugriff auf die eHealth-Plattform über eine integrierte Schnitt-

stelle gewährt, so sind die von den EGD-Gesundheitsdienstleistern verwendeten Praxis- oder Klinikinformationssysteme mittels eines personifizierten Benutzers zu authentifizieren; dabei ist ein dem Stand der Technik entsprechendes Sicherheitsverfahren anzuwenden. Der EGD-Gesundheitsdienstleister hat bei einem Zugriff mittels eines personifizierten Benutzers sicherzustellen, dass der Benutzer sowohl auf Institutions- als auch auf persönlicher Ebene eindeutig identifiziert und protokolliert werden kann. 3) Die technischen Anforderungen an eine Schnittstelle nach Abs. 2 richten sich nach Art. 8 und 9 des Gesetzes und werden vom Amt für Gesundheit auf seiner Internetseite veröffentlicht. EGD-Gesundheitsdienstleister haben dem Amt für Gesundheit auf Verlangen einen Nachweis über die Erfüllung dieser Anforderungen zu erbringen.»

Beschwerde betreffend die Zulässigkeit digitaler Bewerbungsgespräche

Ein Bf brachte bei der DSS Beschwerde ein, dass er im Rahmen eines Bewerbungsverfahrens bei einem liechtensteinischen Unternehmen an einem digitalen Bewerbungsgespräch teilnehmen musste und dieses zudem aufgezeichnet worden sei. Zudem sei sein Auskunftsgesuch gemäss Art. 15 DSGVO nicht rechtmässig beantwortet worden, insbesondere erfolgte keine Übermittlung einer Kopie des Videos.

Die DSS stellte fest, dass online-Bewerbungsgespräche grundsätzlich freiwillig zu erfolgen hätten, als Alternative zu einem Vor-Ort-Gespräch. Dies ergibt sich aus dem Grundsatz der Verhältnismässigkeit und der Datenminimierung in Art. 5 DSGVO. Das verantwortliche Unternehmen bestätigte, dass es die Einwilligung gemäss Art. 7 DSGVO als Rechtsgrundlage vorgesehen und diese auch telefonisch eingeholt hatte. Dazu stellte die DSS fest, dass Art. 7 DSGVO grundsätzlich keine Formvorschriften vorsieht bezüglich des Einholens einer Einwilligung. Dies wird explizit in Erwägungsgrund 32 bestätigt. Anders als Deutschland hat der liechtensteinische Gesetzgeber auch keine Schriftform für die Einholung der Einwilligung eines Arbeitnehmers im nationalen Datenschutzgesetz festgelegt. Nichtsdestotrotz ist bei der Einholung von Einwilligungen im Beschäftigungskontext auf Grund des Machtungleichgewichts grösste Vorsicht geboten. Es muss neben den sonstigen Voraussetzungen in Art. 7 DSGVO insbesondere darauf geachtet werden, dass dem Arbeitnehmer bzw. Bewerber keine Nachteile entstehen, wenn er die Einwilligung nicht gibt.

Die Erfüllung all dieser Voraussetzungen hat der Verantwortliche gemäss Art. 7 Abs. 1 DSGVO nachzuweisen. Im vorliegenden Fall konnte die Bg keinen Nachweis erbringen, da sie die Einwilligung nicht auf schriftlichem Weg, sondern angeblich nur telefonisch eingeholt hat. Nachdem die Parteien widersprüchliche Angaben zum Inhalt des Telefonats und somit zur fraglichen Einwilligung machten, und die Bg keinen Nachweis erbringen konnte, dass sie die Einwilligung vorschriftsgemäss eingeholt hatte, war dem Bf in diesem Beschwerdepunkt recht zu geben und eine Verletzung des Art. 6 Abs. 1 Bst. a iVm Art. 7 DSGVO festzustellen.

Der Bf machte in seiner Beschwerde zudem eine unvollständige bzw. fehlerhafte Auskunft durch die Bg geltend. Insbesondere brachte er vor, dass die Bg ihm keine Kopie des Bewerbungs-Videos sowie interner Notizen habe zukommen lassen. Die Bg brachte dagegen vor, dass es nie zu einer Aufzeichnung des Bewerbungsgesprächs gekommen sei und dass sie zudem, dem Antrag des Bf entsprechend, seine personenbezogenen Daten in Bezug auf die Bewerbung unmittelbar nach Eingang desselben gelöscht habe. Das Gesuch um Auskunft gemäss Art. 15 DSGVO übermittelte der Bf dagegen erst am Folgetag an die Bg , weswegen diesem nicht mehr wie gewünscht nachgekommen werden konnte.

Im vorliegenden Fall hatte die Bg fast zeitgleich beantragte Betroffenenrechte zu gewährleisten, nämlich die zuerst eingegangene Löschanfrage und einen Tag später das Ersuchen um Auskunft. Art. 17 DSGVO verlangt, dass der Verantwortliche die Löschung unverzüglich vornimmt. In Bezug auf die Auskunft im Sinne des Art. 15 DSGVO findet Art. 12 DSGVO Anwendung, welcher bestimmt, dass die Auskunft ebenso wie die anderen Rechte unverzüglich, aber spätestens einen Monat nach Eingang des Antrags, zu erteilen ist. Somit sind gemäss den gesetzlichen Vorgaben beide Rechte innerhalb desselben Zeitrahmens zu erfüllen. Im vorliegenden Fall hat die Bg dem zuerst eingegangenen Antrag entsprechend zuerst die Daten aus dem Bewerbungsverfahren gelöscht und nur die E-Mail-Korrespondenz, deren Löschung eine längere Zeit in Anspruch genommen hat, in der nachfolgenden Auskunftsbeantwortung an den Bf geschickt. Diese Entscheidung kann der Bg nicht zum Vorwurf gemacht werden, da die Löschanfrage zuerst bei ihr eintraf und sie diese pflichtbewusst unverzüglich umsetzte. Die DSS kam daher zum Schluss, dass die Beschwerde betreffend Art. 15 Abs. 1 DSGVO abzuweisen war.

Betreffend die konkrete Frage nach einer Kopie des online-Bewerbungsgesprächs standen ebenfalls widersprüchliche Aussagen im Raum. Der Bf behauptete, es habe eine Aufzeichnung gegeben und legte als Beweis das E-Mail der Mitarbeitenden der Bg vor , welches dies bestätigte. Die Bg erklärte, dass es sich hier um einen Fehler handle, für den sie sich entschuldigte. Die DSS bewertete das Vorbringen der Bg als glaubwür-

dig. Eine Aufzeichnung eines online-Bewerbungsgesprächs wäre unter gewissen, sehr engen Bedingungen (Mifid-Regelungen) zulässig, die jedoch im vorliegenden Fall nicht erfüllt waren, weswegen die Bg letztlich auf eine Aufzeichnung verzichtete. Die DSS kam daher zum Schluss, dass die Beschwerde betreffend Art. 15 Abs. 3 DSGVO (Herausgabe einer Kopie der Aufzeichnung des Gesprächs) abzuweisen war.

Beschwerde betreffend Betroffenenrechte auf Löschung bzw. Rückgabe von Dokumenten

In einem weiteren Beschwerdefall machte eine betroffene Person geltend, dass ihr der ehemalige Arbeitgeber nach Austritt den Strafregisterauszug nicht auf ihr Verlangen zurückgegeben hat.

Die DSS stellte fest, dass die Bf beim Bg das Recht auf Löschung gemäss Art. 17 DSGVO geltend gemacht hatte. Während des Beschwerdeverfahrens stellte sich heraus, dass die verantwortliche Stelle nur sehr unwillig mit der DSS kooperierte und trotz Verwarnung keine Reaktion in Bezug auf das geltend gemachte Betroffenenrecht zeigte. Die DSS verhängte folglich eine Geldbusse in Höhe von CHF 500 für eine Verletzung der Rechenschaftspflicht gemäss Art. 5 Abs. 2 DSGVO. Die Verfügung ist rechtskräftig.

Beschwerde betreffend Auskunftsrecht gemäss Art. 15 DSGVO

Ein Bf brachte bei der DSS eine Beschwerde gegen eine liechtensteinische Bank ein. Darin brachte er vor, er habe als Kunde und ehemaliger Mitarbeiter ein Auskunftsbegehren gemäss Art. 15 DSGVO gestellt. Dieses sei zeitgerecht erfüllt worden, jedoch weitgehend mangelhaft. So bestünden in diversen Bereichen der Bank relevante personenbezogene Daten von ihm, die verarbeitet worden seien und weiterhin verarbeitet würden. Jedoch werde deren Rechtsgrundlage, Verarbeitungszweck und genauer Inhalt nicht offengelegt. Es lasse sich daraus schliessen, dass auch noch weitere, ihm nicht bekannte Daten, unter Vorhalt des Bankgeheimnisses verschwiegen bzw. weiter verarbeitet werden würden.

Die DSS konnte feststellen, dass die Bank dem Bf ein Personaldossier im Sinne einer Kopie gemäss Art. 15 Abs. 3 übermittelt hatte. Nicht umfasst von dieser Auskunft war allerdings eine Information über die in Art. 15 Abs. 1 DSGVO genannten Elemente, weshalb die DSS feststellte, dass die Angaben in Bezug auf die Bst. a, c und d mangelhaft waren. So sind die Verarbeitungszwecke konkret anzugeben – im gegebenen Fall handelt es sich vornehmlich um gesetzlich vorgesehene Speicherverpflichtungen. Des Weiteren steht seit dem Urteil des EuGH vom 12. Januar 2023 (Rechtssache C-154/21) fest, dass die Datenempfänger konkret zu bezeichnen sind. Ein Verweis auf eine Kategorie von Empfängern genügt in den meisten Fällen nicht (mehr). Schliesslich sind die Speicherfristen mit einer konkreten Zeitdauer anzugeben. Nur wenn dies nicht möglich ist, können die Fristen durch Kriterien definiert werden, aus denen sich die Zeitdauer ableiten lässt. Diese drei Elemente wurden nicht ausreichend berücksichtigt, weshalb diesbezüglich eine Verletzung des Art. 15 Abs. 1 Bst. a, c und d DSGVO festzustellen war.

In Bezug auf die Vermutung des Bf, dass wahrscheinlich weitere personenbezogene Daten von ihm bei der Bank verarbeitet würden, musste die DSS feststellen, dass sich dafür aus dem Vorbringen der Bank und des Bf keine konkreten Anhaltspunkte ergaben. Um diesem Verdacht nachgehen zu können, ist die DSS auf konkrete Angaben seitens des Bf angewiesen. Folglich konnte sie keine diesbezügliche Verletzung feststellen.

5.2.2 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 sämtlichen Fällen bestätigte die VBK die Entscheidungen der DSS.

5.2.3 Beschwerden an den Verwaltungsgerichtshof (VGH)

Im Falle einer Verfügung betreffend die Richtigstellung von personenbezogenen Daten gemäss Art. 16 DSGVO erhob die Bf Beschwerde an den VGH. Im Berichtsjahr bestätigte der VGH jedoch die beiden Entscheidungen der DSS und der VBK.

Im Falle einer Verfügung der DSS betreffend die Videoüberwachung einer Freizeitanlage reichte die verantwortliche Stelle eine Beschwerde bei der VBK ein. Gegen die abweisende Entscheidung der VBK erhob die verantwortliche Stelle die Beschwerde an den VGH. Im Dezember 2023 bestätigte der VGH erneut die Entscheidung der DSS. Aufgrund der hohen Relevanz wird diese Entscheidung nachfolgend noch genauer dargestellt.

Der Entscheidung des VGH lag folgender Sachverhalt zu Grunde:

Die Bf betreibt eine grossflächige, öffentlich zugängliche Freizeitanlage im Freien. 2008 wurden auf der Anlage fünf Überwachungskameras installiert, nachdem es zu mehreren Sachbeschädigungen gekommen war. Die fünf Überwachungskameras decken rund 43% der gesamten Anlage ab.

Die DSS entschied mit Verfügung vom 3. November 2021, dass die Videoüberwachung in der Freizeitanlage nicht den Anforderungen der Verhältnismässigkeit, der Datenminimierung und der Zweckbindung gemäss Art. 5 Abs. 1 DSGVO entspricht. Die Bf wurde gemäss Art. 58 Abs. 2 Bst. d DSGVO angewiesen, die Videoüberwachung mit Ausnahme der Kamera 3 (Toiletten) so anzupassen, dass die Aufnahmezeit auf die Zeit der Dämmerung und Dunkelheit beschränkt wird. Weiter wurde die Bf angewiesen, die Speicherdauer grundsätzlich auf 72 Stunden zu reduzieren. Bei verlängerten Wochenenden und Ferienabwesenheiten konnte die Speicherdauer entsprechend angepasst werden. Ausserdem wurde die Bf angewiesen, der Informationspflicht nach Art. 13 DSGVO nachzukommen und der DSS die Umsetzung der angeordneten Massnahmen bis zum 6. Dezember 2021 nachzuweisen.

Gegen die Verfügung der DSS erhob die Bf Beschwerde an die VBK. Mit Entscheidung vom 30. November 2022 wies die VBK die Beschwerde gegen die Verfügung der DSS ab.

Gegen diese Entscheidung der VBK erhob die Bf Beschwerde an den VGH. Der VGH zog die Vorakten der DSS und der VBK bei, erörterte in nichtöffentlicher Sitzung am 15. Dezember 2023 die Sach- und Rechtslage und wies die Beschwerde ebenfalls ab.

Aus den Entscheidungsgründen:
Strittig und Gegenstand des vorliegenden Beschwerdeverfahrens vor dem VGH ist allein die Frage, ob keine die Videoüberwachung zumutbar ist, d.h. ob keine schutzwürdige Interessen der Betroffenen die berechtigten Interessen der Bf überwiegen.

Die DSS, bestätigt durch die VBK, ist der Ansicht, dass die schutzwürdigen Interessen der Betroffenen tagsüber überwiegen und die von der Bf betriebene Videoüberwachung bei Tageslicht somit unzumutbar ist. Bei der Überwachung von Personen, die einer Freizeittätigkeit nachgehen, sind besondere Anforderungen zu beachten. Die Freizeitanlage wird nicht nur als Durchgang genutzt, sondern von Personen zur Freizeitausübung aufgesucht. Die Nutzung des Platzes ist nur tagsüber vorgesehen, da keine Flutlichtanlage vorhanden ist. Die unüberwachte Freizeitgestaltung ist ein hohes Gut, das im Rahmen einer Verhältnismässigkeitsprüfung besonders berücksichtigt werden sollte. Bei dieser Prüfung müssen die Interessen der Betroffenen besonders gewichtet werden. Daher sollte eine zeitliche Begrenzung für den Betrieb der Videokameras festgelegt werden. Die Aufnahmezeit sollte auf die dunkle Tageszeit beschränkt werden.

Dem Argument der Bf, die Aufzeichnungen seien in zeitlicher Hinsicht dadurch begrenzt, dass durch einen Bewegungsmelder nur eingeschränkt Daten erhoben würden, folgt der VGH nicht. Das Argument, es handele sich bei der Videoüberwachungsanlage um eine «Black-Box»-Lösung, weist er mit der Begründung zurück, dass die aufgezeichneten Bilder nicht ausschliesslich auf einem Datenspeicher gespeichert und in der Regel nach einem bestimmten Zeitintervall automatisch überschrieben werden. Stattdessen werden die Videoaufnahmen auf einen Live-Monitor übertragen, so dass die Möglichkeit besteht, die Bilder live einzusehen. Der VGH ist der Auffassung, dass diese Vorgehensweise jedenfalls nicht zu einer Minimierung des Eingriffs in die Rechte der Betroffenen führt.

Der VGH weist auch das Vorbringen der Bf zurück, wonach nur 43% des Freizeitgeländes von den Videokameras erfasst würden, da dies nichts daran ändere, dass die Datenerhebung in die Persönlichkeitsrechte der Personen eingreife, die auf dem Freizeitgelände Freizeitaktivitäten ausüben. Die staatliche Überwachung des Freizeitverhaltens der Bevölkerung stellt einen schwerwiegenden Eingriff dar; auf einen prozentualen Anteil kommt es hierbei nicht an.

Dem weiteren Vorbringen der Bf, eine Beschränkung der Aufnahmezeiten auf Dämmerung und Dunkelheit sei unverhältnismässig, weil sich die Schadensfälle bei Tageslicht ereignet hätten und somit eine erhebliche Anzahl von Schadensfällen voraussichtlich nicht aufgeklärt werden könne, hält der VGH entgegen, dass die von der Bf verfolgten Interessen hinter den Interessen der Betroffenen zurückzutreten haben, wenn wie oben festgestellt Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (Art. 5 Abs. 1 Bst. b DSG).

In Bezug auf das Argument der Bf, dass die Videoüberwachung auch dem Schutz der Besucher des Freizeitareals diene, hält ihr der VGH entgegen, dass sie nicht darlegt, inwieweit eine erhöhte Gefahr für Leib und Leben der Besucher besteht. Selbst wenn eine gewisse Gefahr für die Besucher bestünde, ist keinesfalls ersichtlich, dass diese Gefahr eine Schwere aufweist, die den Anwendungsbereich des § 5 Abs. 2 DSG eröffnen und eine Videoüberwachung rechtfertigen könnte.

In der Gesamtabwägung der berechtigten Interessen der Bf einerseits und der Intensität des Eingriffs in die Rechte der Betroffenen andererseits bestätigt der VGH die Entscheidung der DSS, indem er die Videoüberwachung des Freizeitareals bei Tageslicht – mit Ausnahme der Überwachung des Eingangsbereichs der Toilettenanlage – als nicht zumutbar und damit als nicht gerechtfertigt erachtet.

5.2.4 Beschwerden an den Staatsgerichtshof (StGH)

Im Falle der vom VGH entschiedenen Beschwerde betreffend die Geltendmachung des Berichtigungsrechts nach Art. 16 DSGVO erhob die Bf Individualbeschwerde an den StGH.

5.3 Meldung von Datenschutzverletzungen gemäss Art. 33 DSGVO

Art. 33 DSGVO sieht vor, dass Verletzungen des Schutzes personenbezogener Daten der zuständigen Datenschutz-Aufsichtsbehörde binnen 72 Stunden zu melden sind, wenn aufgrund der Verletzung voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Die betroffenen Personen müssen gemäss Art. 34 DSGVO ebenfalls unverzüglich benachrichtigt werden, wenn voraussichtlich ein hohes Risiko für ihre Rechte und Freiheiten zu erwarten ist.

2023 erhielt die DSS 56 Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO, wovon in 20 Fällen die betroffenen Personen über die Datenschutzverletzung benachrichtigt wurden (Art. 34 DSGVO). Dies bedeutete eine Zunahme von 40% im Vergleich zum Vorjahr, in dem 40 Meldungen nach Art. 33 DSGVO erfolgten. Zusätzlich nahmen auch die Fälle deutlich zu, in denen die Betroffenen zu informieren waren. Die zunehmenden Benachrichtigungen gemäss Art. 34 DSGVO zeigen, dass die Schwere der Fälle signifikant zugenommen hat. Obwohl immer mehr Verantwortliche bereit sind, umfassend über Datenschutzverletzungen zu informieren, stellte die Frage der Benachrichtigung der Betroffenen auch im Berichtsjahr in einigen Fällen eine komplexe Angelegenheit dar, die einen umfangreichen Beratungsaufwand seitens der DSS erforderte.

Insgesamt zeigten die Meldungen, 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 von Banken, Versicherungen, Telekommunikationsbetrieben, Gewerbe und Treuhandunternehmen. Nicht selten waren einfachste und bereits seit langem bekannte Sicherheitsmängel bzw. -fehler der Grund für die Datenpannen, weshalb davon auszugehen ist, dass die Dunkelziffer der tatsächlich erfolgten Pannen noch um einiges höher ist.

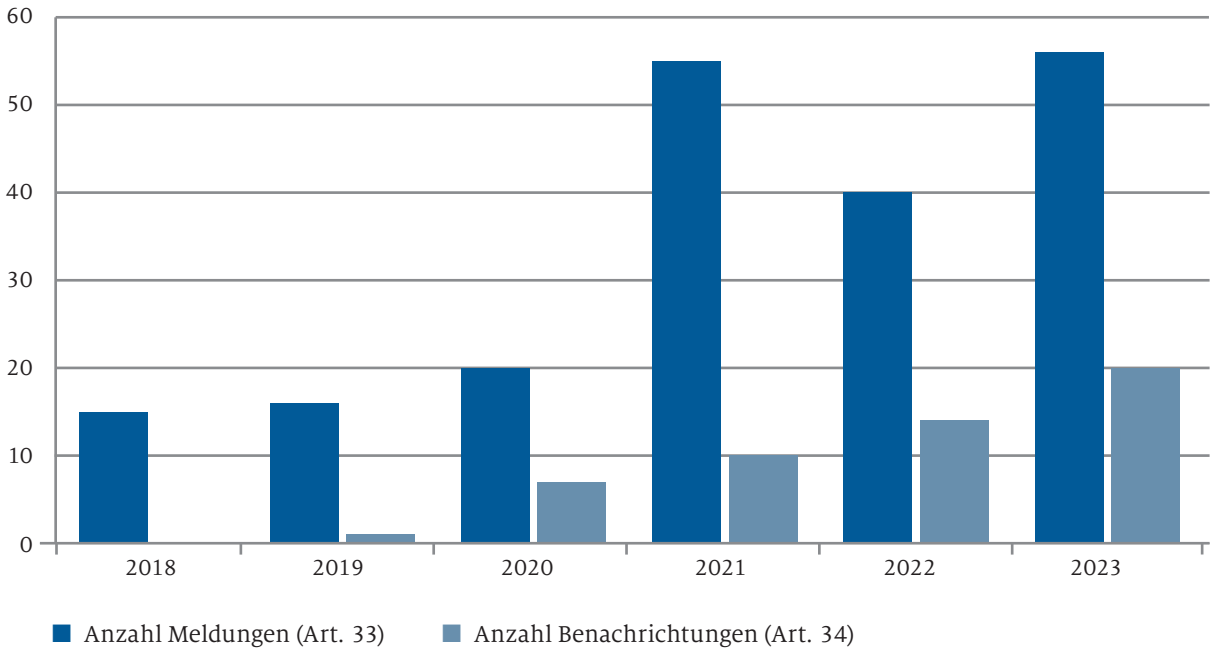
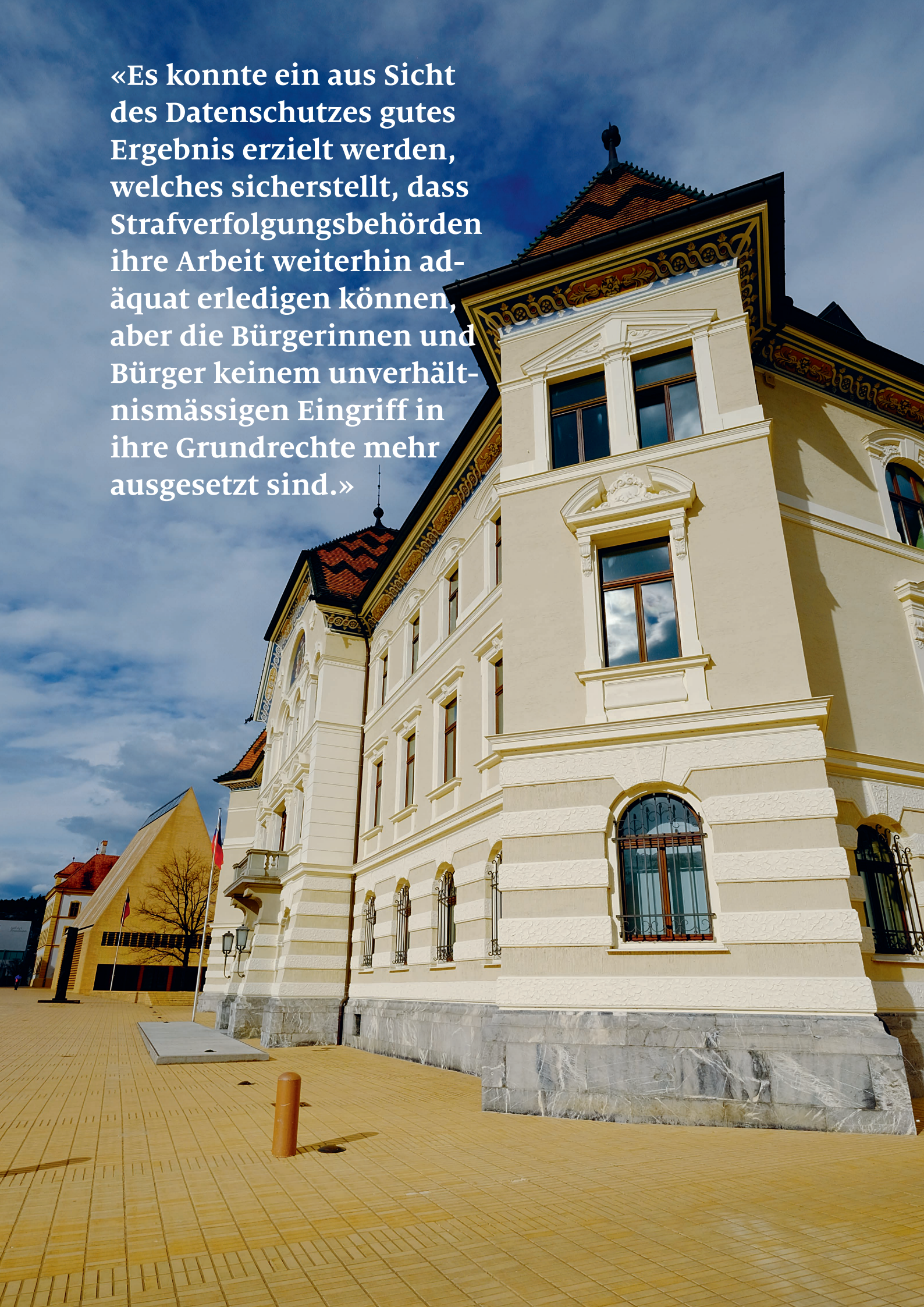


Abbildung 6: Anzahl der gemeldeten Datenschutzverletzungen pro Jahr



«Es konnte ein aus Sicht des Datenschutzes gutes Ergebnis erzielt werden, welches sicherstellt, dass Strafverfolgungsbehörden ihre Arbeit weiterhin adäquat erledigen können, aber die Bürgerinnen und Bürger keinem unverhältnismässigen Eingriff in ihre Grundrechte mehr ausgesetzt sind.»

6. Mitarbeit in Arbeitsgruppen, Projekten und Kommissionen der Landesverwaltung

6.1 Ratifikation Konvention 108+

Die DSS hat im Berichtsjahr weiterhin das Amt für Auswärtige Angelegenheiten beim Ratifikationsprozess des Änderungsprotokolls zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) des Europarats unterstützt. Das Übereinkommen wurde kürzlich mittels eines Änderungsprotokolls modernisiert und insbesondere an die heutigen informations- und kommunikationstechnologischen Möglichkeiten der Datenverarbeitung angepasst. Die formelle Ratifikation des Änderungsprotokolls durch Liechtenstein erfolgte am 17. Mai 2023 anlässlich des Gipfeltreffens des Europarats in Reykjavík. Insgesamt sind 38 Ratifikationen erforderlich, damit das Änderungsprotokoll bzw. die modernisierte Konvention 108+ in Kraft treten kann. Das Erreichen dieser Marke wird für 2024 erwartet.

6.2 Modern Workplace

Im Rahmen des LLV-Projekts Modern Workplace, welches im Wesentlichen die schrittweise Einführung von Microsoft 365-Diensten umfasst, wurde die DSS ersucht, Einsitz im Fachausschuss zu nehmen. Im Oktober fand die erste Sitzung des Fachausschusses statt. Initial wurde den Mitgliedern der Projektplan vorgestellt. Aufgrund von Projektverzögerungen und Anpassungen des ursprünglichen Projektumfangs werden die nächsten Sitzungen des Fachausschusses erst im Jahr 2024 erfolgen.

6.3 Vorratsdatenspeicherung

Die liechtensteinischen Bestimmungen zur Vorratsdatenspeicherung wurden 2010 im Gesetz über die elektronische Kommunikation (KomG) sowie der Verordnung über elektronische Kommunikationsnetze und -dienste (VKND) eingeführt. Damit wurden die Vorgaben der in das EWR-Abkommen übernommenen Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der vom EuGH zwischenzeitlich für ungültig erklärten Richtlinie 2006/24/EG (Richtlinie über die Vorratsspeicherung von Daten) umgesetzt. Weiter stellte der EuGH in mehreren Urteilen fest, dass die Grundrechtecharta der Europäischen Union dahingehend auszulegen sei, dass diese einer nationalen Rechtsvorschrift, die für die Zwecke der Verfolgung schwerer Straftaten oder zur Abwehr einer konkreten Gefahr der nationalen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung eines Grossteils der Verkehrs- und Standortdaten mit einer Speicherungsfrist von mehreren Wochen vorsehe, entgegenstehe. Ausnahmen hierzu können gemäss EuGH in Bezug auf die Speicherung von IP-Adressen und Daten zur Identifikation von Teilnehmern vorgesehen werden. Die Urteile des EuGH sind insofern für Liechtenstein von Bedeutung, als die in der Grundrechtecharta der Europäischen Union normierten Grundrechte weitgehend identisch mit den von der liechtensteinischen Verfassung und der in Liechtenstein anwendbaren Europäischen Menschenrechtskonvention normierten Grundrechten sind und die Urteile somit weitgehend auch auf die liechtensteinischen Verhältnisse übertragbar sind. Vor diesem Hintergrund setzte die Regierung unter dem Vorsitz des Amtes für Kommunikation eine Arbeitsgruppe aus Vertretern des Amtes für Justiz, der DSS, der Landespolizei, des Fürstlichen Landgerichtes und der Staatsanwaltschaft ein und beauftragte diese, die geltende Regelung zur Vorratsdatenspeicherung zu überprüfen. Diese Entscheidung begrüsste die DSS sehr, hatte sie in den letzten Jahren doch mehrfach auf die Problematik der Vorratsdatenspeicherung hingewiesen.

Nach einigen sehr kooperativen und produktiven Arbeitssitzungen konnte ein aus Sicht des Datenschutzes gutes Ergebnis erzielt werden, welches sicherstellt, dass Strafverfolgungsbehörden ihre Arbeit weiterhin adäquat erledigen können, aber die Bürgerinnen und Bürger keinem unverhältnismässigen Eingriff in ihre Grundrechte mehr ausgesetzt sind.

6.4 Beratung zu weiteren Gesetzgebungsprozessen

Zusätzlich zu den genannten Beratungen unterstützte die DSS auch weitere Stellen bei Einzelfragen in verschiedenen Gesetzgebungsprozessen (z.B. Umsetzung Richtlinie (EU) 2021/1232, Durchführung Verordnung (EU) 2018/1807, Revision StPV).

6.5 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. Dieser obliegt die Entscheidung über die Offenlegungsanträge Dritter im Sinne von Art. 17 VwbPG. 2023 wurden zwei Anträge betreffend die Offenlegung von Daten an Dritte an das Amt für Justiz gestellt. Beide Anträge wurden 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 all 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 2023 an den meisten Sitzungen der Arbeitsgruppen teilnehmen und aktiv mitarbeiten. Die DSS nahm ausserdem an sämtlichen 15 Plenarsitzungen des Ausschusses teil.

Der EDSA hat im Jahr 2023 auf Grundlage des Art. 64 Abs. 1 DSGVO insgesamt **35 Stellungnahmen** zu Vorlagen von nationalen Datenschutz-Aufsichtsbehörden abgegeben. Darunter fielen:

- vier Stellungnahmen zu je einem Entscheidungsentwurf bezüglich der Akkreditierungsanforderungen für eine Stelle zur Überwachung von Verhaltensregeln gemäss Art. 41 DSGVO (Kroatien, Lettland, Rumänien, Schweden);
- drei Stellungnahmen zu je einem Entscheidungsentwurf bezüglich der Akkreditierungsanforderungen für eine Zertifizierungsstelle gemäss Art. 43 Abs. 3 DSGVO (Kroatien, Malta, Zypern);
- eine Stellungnahme zum Entscheidungsentwurf bezüglich die Brand Compliance Zertifizierungskriterien (Niederlande);
- zahlreiche Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (American Express Global Business Travel Group, zwei zu Autodesk Group, Booking.com Group, Carlsberg Group, zwei zu Cerner Group, Collibra Group, Comcast Corporation Group, zwei zu Informatica Group, Nestlé Group, OSF Global Services Group, PROSEGUR Group, Royal Greenland Group, Servier Group, SHV Holding N.V. Group, zwei zu Sodexo Group, Tessi Group, zwei zu Thalès Group, drei zu UPS Group, Vertiv, Vestas Wind Systems Group).

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

- Stellungnahme zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Schutzes personenbezogener Daten im Rahmen des Datenschutzrahmens EU-USA.

Daneben haben der EDSA und der Europäische Datenschutzbeauftragte (EDSB) 2023 auch zwei **Gemeinsame Stellungnahmen** erlassen:

- Gemeinsame Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679;
- Gemeinsame Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einführung des digitalen Euro.

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

- Anwendung des Artikels 65(1)(a) DSGVO, Version 2.0 (EDPB Guidelines 03/2021);
- Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO, Version 2.0 (EDPB Guidelines 05/2021);
- Betroffenenrechte – Recht auf Auskunft, Version 2.0 (EDPB Guidelines 01/2022);
- «Dark Patterns» bei Benutzerschnittstellen von Plattformen Sozialer Medien: Wie man sie erkennt und vermeidet, Version 2.0 (EDPB Guidelines 03/2022);
- Berechnung von Geldbussen im Sinne der DSGVO, Version 2.1 (EDPB Guidelines 04/2022);
- Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung, Version 2.0 (EDPB Guidelines 05/2022);
- Zertifizierung als Instrument für Übermittlungen, Version 2.0 (EDPB Guidelines 07/2022);
- Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters, Version 2.1 (EDPB Guidelines 08/2022);
- Meldung von Datenschutzverletzungen nach der DSGVO, Version 2.0 (EDPB Guidelines 09/2022).

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

- zu Artikel 37 der Strafverfolgungsrichtlinie (EDPB Guidelines 01/2023);

– zum technischen Anwendungsbereich von Art. 5(3) der Datenschutzrichtlinie für elektronische Kommunikation (EDPB Guidelines 02/2023).

Im Berichtsjahr wurde vom EDSA ausserdem eine **Empfehlung** zu folgendem Thema **angenommen**:

– Genehmigungsantrag sowie Elemente und Grundsätze, die in den Verbindlichen internen Datenschutzvorschriften eines Verantwortlichen enthalten sein müssen (Art. 47 DSGVO) (Empfehlung 01/2022).

7.1.1 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, Task Forces) zu ganz unterschiedlichen Themen Einsitz, welche nachfolgend dargestellt werden. Die Mitarbeitenden der DSS haben 2023 an insgesamt 131 Sitzungen des Ausschusses und solcher Arbeitsgruppen digital oder vor Ort teilgenommen.

Die spezielle Arbeitsgruppe (Task Force) des EDSA zu Bussgeldern gemäss DSGVO *(Taskforce Fining)* befasst sich mit der konkreten Berechnung solcher Bussgelder und strebt europaweit eine möglichst einheitliche Herangehensweise an. Nachdem 2022 die offiziellen Leitlinien des EDSA zum Thema verabschiedet wurden, hat die Task Force im Berichtsjahr noch eine ergänzende Tabelle zu den Leitlinien ausgearbeitet. Darin werden die Ausführungen und Berechnungsvorgaben der Leitlinien zusätzlich tabellarisch dargestellt, womit einem entsprechenden Bedürfnis nachgekommen wurde. Auch das zentrale Bussgeldregister des EDSA wurde im Berichtsjahr einer Überarbeitung unterzogen und die Methode zur Bussgeldberechnung beim gleichzeitigen Vorliegen mehrerer Verstösse gegen die DSGVO weiter diskutiert (Art. 83 Abs. 3 DSGVO). Daneben wurde die Arbeit an einem Dokument zu Best Practices der Behörden bei Bussgeldentscheiden aufgenommen.

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 Verfahren im Rahmen des Streitbeilegungsmechanismus gemäss Art. 65 DSGVO beschäftigt. Zahlreiche betroffene Aufsichtsbehörden hatten massgebliche und begründete Einsprüche gegen die Beschlussentwürfe der federführenden Aufsichtsbehörde eingelegt, denen sich diese jedoch nicht angeschlossen bzw. welche diese abgelehnt hatte. Der in solchen Fällen erforderliche verbindliche Beschluss des EDSA zur Streitbeilegung wurde von der Arbeitsgruppe für zwei Verfahren vorbereitet. Dazu kam die Vorbereitung eines verbindlichen Beschlusses des EDSA in einem Dringlichkeitsverfahren gemäss Art. 66 DSGVO. Ausserdem erarbeitete die Arbeitsgruppe ein Template für die Einreichung von massgeblichen und begründeten Einsprüchen gegen Beschlussentwürfe.

Wertvoll aus Sicht der DSS war darüber hinaus auch 2023 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 ausserdem über Verfahren und Entscheidungen im Bereich Datenschutz Minderjähriger diskutiert.

Sodann hat die Arbeitsgruppe weiter am Projekt zum Recht auf rechtliches Gehör im Rahmen datenschutzrechtlicher Verfahren gearbeitet, woran die DSS als Co-Rapporteur beteiligt ist. Ausserdem wurden die Arbeiten der *Taskforce 101* und der *Cookie Banner Taskforce* fortgeführt. 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 und legte im Berichtsjahr ihren abschliessenden Bericht vor. Die *Cookie Banner Taskforce* behandelte diverse Fragen rund um die rechtlich zulässige oder unzulässige Gestaltung von Cookie-Bannern. Sie hat ihren abschliessenden Bericht anfangs 2023 publiziert.

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

Im Berichtsjahr wurde eine solche *Coordinated Action* zum Thema der Stellung und der Rolle von betrieblichen Datenschutzbeauftragten durchgeführt. Die DSS hat sich daran beteiligt und mittels eines umfangreichen Fragebogens an alle gemeldeten betrieb-

lichen Datenschutzbeauftragten in Liechtenstein Informationen darüber erhoben, wie sie ernannt werden, über welche Ausbildung und Weiterbildungsmöglichkeiten sie verfügen, wieviele Ressourcen ihnen für die Erledigung ihrer Aufgaben zur Verfügung stehen, wie sie in datenschutzrelevante Fragestellungen in ihren jeweiligen Organisationen einbezogen werden, an wen sie rapportieren etc. Die Antworten hat die DSS in einem nationalen Bericht zusammengefasst und den Datenschutzbeauftragten am Vernetzungstreffen im Herbst 2023 präsentiert. Der über alle teilnehmenden Behörden aggregierte Abschlussbericht ist vom EDSA anfangs 2024 auf europäischer Ebene veröffentlicht worden. Durch die im Rahmen dieser koordinierten Aktion gewonnenen Erkenntnisse kann die DSS die betrieblichen Datenschutzbeauftragen in Liechtenstein künftig noch besser unterstützen, indem sie für diese zielgerichtete Weiterbildungen, Informationen und Beratung anbieten kann.

Für 2024 wurde bereits wieder eine neue *Coordinated Action* lanciert, welche sich mit der Umsetzung des Auskunftsrechts von Betroffenen gemäss Art. 15 DSGVO befasst.

In der Arbeitsgruppe, welche sich mit der Zusammenarbeit der Aufsichtsbehörden befasst *(Cooperation Subgroup)*, wurde im Berichtsjahr gemeinsam mit dem Europäischen Datenschutzbeauftragten eine Stellungnahme zum Gesetzgebungsvorschlag der EU-Kommission für weitere harmonisierte Verfahrensregelungen zur Durchsetzung der DSGVO erarbeitet. Zudem wurde die Arbeit an einer Guidance für die Vereinfachung der Behandlung grenzüberschreitender Fälle weitergeführt und die Überarbeitung der Leitlinien zu Art. 60 DSGVO und zu Art. 61 DSGVO gestartet. Darüber hinaus wurde die Arbeit an einem gemeinsamen europäischen Register der Vertreter gemäss Art. 27 DSGVO von Organisationen aus Drittstaaten weitergeführt sowie ein gemeinsames europäisches Beschwerdeformular für betroffene Personen geschaffen. Schliesslich wurde die Diskussion über die Anwendung bzw. Nicht-Anwendung des One-Stop-Shop Mechanismus (formelle Zusammenarbeit der Datenschutzbehörden in grenzüberschreitenden Fällen) eröffnet, in Situationen, in denen nationales Recht involviert ist (Art. 55 DSGVO).

Die thematische Arbeitsgruppe zu Finanzangelegenheiten des EDSA *(Financial Matters Subgroup)* hat im Berichtsjahr weiterhin einen aktiven Austausch mit der Europäischen Zentralbank zum voranschreitenden Projekt der Einführung eines Digitalen Euros geführt und gemeinsam mit dem Europäischen Datenschutzbeauftragten eine Stellungnahme zu den entsprechenden gesetzlichen Regelwerken erarbeitet. Darüber hinaus hat sie an die Kommission eine weitere Stellungnahme zur Revision der Gesetzgebung über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung abgegeben sowie die Erarbeitung entsprechender Leitlinien zum Thema lanciert. Daneben hat sie auch wieder diverse Diskussionen geführt sowie kleinere Beiträge und Stellungnahmen erarbeitet zu Themen wie PSD3, FATCA, Mobile Payments, zwingende Nutzerkontoeröffnung in Online-Shops, Open Finance oder zur Revision der Konsumkreditrichtlinie. Viele dieser Arbeiten werden auch 2024 fortgeführt. Zudem wurde eine *Taskforce Competition and Consumer Law* zur Untersuchung der Zusammenhänge zwischen Datenschutz und Wettbewerbsrecht gegründet, welche im Berichtsjahr die Arbeit aufgenommen hat.

Die Arbeitsgruppe zu Fragen bezüglich Datenübermittlungen in Drittstaaten *(International Transfer Subgroup)* hat im Berichtsjahr die Arbeiten an der Leitlinie über Zertifizierungen als geeignete Garantien und den Leitlinien über das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO abgeschlossen. Letztere geben insbesondere Aufschluss darüber, was unter einem Datentransfer zu verstehen ist. Weiters wurden im Berichtsjahr zwei Workshops zu Zertifizierungen (auch in Zusammenhang mit internationalen Datenübermittlungen) durchgeführt. Die DSS nahm an diesen Workshops nicht teil, da Zertifizierungen in Liechtenstein zurzeit gar nicht möglich sind. Auch die Kooperation der EU-Kommission mit den amerikanischen Vertretern zur Etablierung eines neuen Rechtsrahmens, der den EU-U.S.-Datentransfer (wieder) rechtlich möglich machen soll, wurde von der Arbeitsgruppe beobachtet. Sie erhielt regelmässige Informationen durch die EU-Kommission und bereitete eine Stellungnahme des EDSA zu Handen der EU-Kommission zur Angemessenheitsentscheidung «EU-U.S. Data Privacy Framework» vor. Ein weiterer Angemessenheitsbeschluss, der die Arbeitsgruppe im Berichtsjahr beschäftigte, war jener betreffend Japan. Nach einem Zeitraum von zwei Jahren wurde dieser durch die EU-Kommission einer Überprüfung unterzogen. Im April des Berichtsjahres wurde diese abgeschlossen. Die Arbeitsgruppe bereitete dafür eine Stellungnahme des EDSA vor. Auch BCR-Verfahren beschäftigten die Arbeitsgruppe in vielerlei Hinsicht. So wurden immer wieder inhaltliche Fragestellungen und Zuständigkeitsfragen aufgeworfen. Weiters galt es den Genehmigungsprozess zu organisieren betreffend aller Verfahren, die noch die alte Hilfestellung (Working-Paper 256) als Grundlage genutzt hatten, denn diese mussten noch im Berichtsjahr mit einer Stellungnahme des EDSA abgeschlossen werden. Zusätzlich wurden interne Vorlagen, Internetseiten

und Prozesse umgestaltet und überarbeitet. Im letztjährigen Tätigkeitsbericht wurde an dieser Stelle über die Überarbeitung der Hilfestellung der sogenannten «Controller BCR» (Verbindliche interne Datenschutzvorschriften für Verantwortliche) informiert. Diese konnten im Berichtsjahr endgültig abgeschlossen werden. Neben «Controller BCR» gibt es auch sogenannte «Processor BCR» (Verbindliche interne Datenschutzvorschriften für Auftragsdatenverarbeiter). Im Berichtsjahr wurde, gestützt auf die Arbeiten bezüglich der Überarbeitung der Hilfestellung für «Controller BCR», damit begonnen, auch die Hilfestellung für «Processor BCR» (Working-Paper 257) zu überarbeiten. Eine Arbeitsgruppe wurde gebildet, welche am Ende des Berichtjahres einen ersten Entwurf vorstellen konnte. Erfahrungsgemäss wird es jedoch noch einige weitere Diskussionen bis zur Finalisierung geben, so etwa über die Frage wie und ob die Elemente eines Auftragsverarbeitungsvertrages (Art. 28 DSGVO) in die «Processor BCR» aufgenommen werden können.

Die CEH-Arbeitsgruppe *(CEH Expert Subgroup),* eine Kurzbezeichnung für Compliance, E-Government und Health, befasste sich auch in diesem Jahr mit den ihr zur Vorprüfung unterbreiteten Akkreditierungskriterien für Überwachungsstellen nach Art. 41 DSGVO und Akkreditierungskriterien für Zertifizierungsstellen nach Art. 43 DSGVO von verschiedenen Mitgliedstaaten, zu denen der EDSA nachfolgend eine Stellungnahme verfassen sollte. Ebenfalls beschäftigte sich die Arbeitsgruppe mit den unterbreiteten Zertifizierungskriterien von Brand Compliance, welche dem EDSA von der niederländischen Datenschutzaufsichtsbehörde zur Stellungnahme gemäss Art. 64 Abs. 1 Bst. c DSGVO unterbreitet worden waren.

Im Gesundheitsbereich widmete sich die Arbeitsgruppe einigen Detailfragen zu den Leitlinien zur Verarbeitung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung. Besondere Herausforderungen bildeten dabei die Unterschiede in der Herangehensweise an die wissenschaftliche Forschung in den Mitgliedstaaten und die daraus resultierenden Auswirkungen auch auf die Leitlinien.

Ein weiterer Schwerpunkt war 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 etwa Workshops in diesem Bereich angeboten.

Die Arbeitsgruppe zu technologischen Themen *(Technology Expert Subgroup)* befasste sich im Jahr 2023 ebenfalls mit einem breiten Themenspektrum und erarbeitete mehrere Leitlinien, Empfehlungen und Stellungnahmen für den EDSA.

Die EU-Kommission veröffentlichte am 11. Mai 2022 einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern. Trotz zahlreicher Verhandlungen zwischen den EU-Mitgliedstaaten konnte im Rat der Europäischen Union im Jahr 2023 keine Einigung über einen gemeinsamen Standpunkt zu diesem Vorschlag erzielt werden. Der von der Arbeitsgruppe erarbeitete Vorschlag für eine Leitlinie über den Einsatz von Technologien zur Aufdeckung und Meldung von sexuellem Kindesmissbrauch im Internet wurde im Jahr 2023 auf der Grundlage der aus den Verhandlungen resultierenden legislativen Entwicklungen überarbeitet und dem Ausschuss zur Verabschiedung vorgelegt. Ein Beschluss zur Verabschiedung der Leitlinie konnte bislang nicht gefasst werden, so dass davon auszugehen ist, dass eine Entscheidung über das weitere Vorgehen in Bezug auf die Leitlinie im ersten Halbjahr 2024 ansteht. Als Reaktion auf die legislativen Entwicklungen hat die Arbeitsgruppe auch eine Stellungnahme des EDSA vorbereitet, die voraussichtlich im ersten Halbjahr 2024 veröffentlicht wird.

Sowohl die Leitlinie zur Anonymisierung als auch die Leitlinie zur Pseudonymisierung sind noch in Ausarbeitung. Unter anderem aufgrund der möglichen Auswirkungen der Entscheidung des Gerichts der Europäischen Union (EuG) in der Rechtssache T-557/20 und des damit verbundenen Berufungsverfahrens auf die Leitlinien wird deren Anpassung und Verabschiedung durch den Ausschuss noch einige Zeit in Anspruch nehmen.

Weitere Tätigkeiten der Arbeitsgruppe im Berichtsjahr umfassten die Initiierung einer Leitlinie zum Zusammenspiel zwischen dem EU-Gesetz über künstliche Intelligenz (AI-Act) und der DSGVO, den Austausch mit anderen Behörden sowie den Informationsaustausch zwischen verschiedenen Arbeitsgruppen des EDSA, um nur einige Beispiele zu nennen.

Die Arbeitsgruppe zu Sozialen Medien *(Social Media Subgroup)* legte ihren Fokus im Jahr 2023 auf die Ausarbeitung der Richtlinie zur Nutzung sozialer Medien durch öffentliche Stellen. Bis Ende 2023 konnte die Arbeit zwar noch nicht abgeschlossen werden, jedoch ist der Reifegrad des Dokuments sehr weit fortgeschritten. Des Weiteren wird Anfangs 2024 eine Mandatsanfrage an das Plenum des EDSA gestellt werden betreffend die Ausarbeitung einer Leitlinie über das Zusammenspiel zwischen dem Gesetz über digitale Dienste (Digital Services Act (DSA)) und der DSGVO. In der EU wird die Verordnung ab dem 17. Februar 2024 volle Wirksamkeit entfalten. Für die sogenannten sehr grossen Online-Plattformen und Online-Suchmaschi-

nen mit mehr als 45 Millionen Nutzern in der EU (10% der EU-Bevölkerung) gelten diese Vorschriften bereits seit Ende August 2023.

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.

Die BTLE-Arbeitsgruppe *(BTLE Expert Subgroup)* konnte mangels Ausscheiden des zuständigen Mitarbeitenden im Berichtsjahr von der DSS nicht betreut werden.

7.1.2 Workshop Webseiten-Prüfwerkzeuge

Der EDSA organisierte im Juni 2023 einen Workshop für die Datenschutzbehörden, bei dem Werkzeuge für die Inspektion von Internetseiten vorgestellt wurden. Im Fokus standen die Anwendung der Werkzeuge bzw. Programme sowie der Informationsaustausch unter den Behörden. Beide Programme (Website Evidence Collector sowie Website Auditing Tool) sind für Windows, MacOS, sowie Linux öffentlich verfügbar. Für Interessierte ist es somit möglich, einen Webseitencheck hinsichtlich Cookies, Skripts, Verkehrsanalyse etc. durchzuführen. Der Website Evidence Collector wurde federführend vom Europäischen Datenschutzbeauftragten entwickelt und erfordert für die Anwendung gute IT-Kenntnisse. Die zweite Anwendung wurde im Rahmen eines internen Projekts des EDSA entwickelt und ist für ein breiteres Zielpublikum gedacht. Der fruchtbare Austausch fand während zwei Tagen statt. Für 2024 hat der EDSA bereits zusätzliches Budget für die Weiterentwicklung des Website Auditing Tools zur Verfügung gestellt.

7.1.3 Gegenseitige Amtshilfe

Die DSGVO erfordert neben der Zusammenarbeit der europäischen Datenschutz-Aufsichtsbehörden im bzw. mit dem EDSA auch eine intensive Kommunikation zwischen den einzelnen Aufsichtsbehörden, indem diese gemäss Art. 57 Abs. 1 Bst. g DSGVO «mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten». Die DSS erhielt im Berichtsjahr 195 Anfragen von anderen europäischen Datenschutzaufsichtsbehörden, was im Vergleich zu den im Vorjahr beantworteten 78 Anfragen eine sehr starke Zunahme bedeutete. Die Anfragen wurden jeweils gestellt, wenn im Vollzug der aufsichtsrechtlichen Tätigkeit Interpretationsspielraum bestand und die anfragende Datenschutzaufsichtsbehörde die Rechtsmeinung anderer Aufsichtsbehörden bzw. die Anwendung von Bestimmungen der DSGVO durch andere Mitgliedstaaten erfahren wollte. Die Anfragen betrafen unter anderem folgende Themen: Handel, Miete und Verkauf von personenbezogenen Daten; Direktwerbung (b2b); Parkplatz Apps; Tracking-Pixels; Benutzung von Dashcams; Videoüberwachung von öffentlichen Plätzen und in öffentlichen Räumen sowie Audioaufzeichnungen in Schulen und Klassenzimmern; Streaming von Jugendsportveranstaltungen; Videoüberwachungssysteme mit Gesichtserkennung; Videoüberwachungen in kritischen Infrastruktureinrichtungen; Aufzeichnung von Verarbeitungstätigkeiten; Datentransfer in ein Drittland; Umsetzung der Richtlinie zur Netzwerk- und Informationssicherheit (NIS2).

Insgesamt lässt sich in Bezug auf diese Amtshilfeersuchen feststellen, dass sie ebenso wie die allgemeinen Anfragen an die DSS an Komplexität zunahmen und vielfach Fragen des Datenschutzes im Rahmen neuer Technologien betrafen.

7.2 Gemeinsame Massnahmen der Aufsichtsbehörden gemäss Art. 62 DSGVO

Der EDSA beschloss bereits 2022 eine länderübergreifende strategische Untersuchung zum Thema SmartTV zu starten. Da die DSS durchaus einen Mehrwert für das Thema erkannte, sagte sie ihre Unterstützung zu. Nach diversen vorbereitenden Massnahmen reisten zwei technische Experten der DSS dazu im September 2023 nach Den Haag, um die niederländische Datenschutzbehörde vor Ort bei der technischen Untersuchung unterstützen zu können. Neben der niederländischen Behörde beteiligen sich auch die italienischen und ungarischen Kollegen an der Untersuchung. Da in einigen der Länder Beschwerdeverfahren hängig sind, können zu diesem Zeitpunkt keine Details zu der Untersuchung genannt werden. Nach dem Abschluss der offiziellen Verfahren wird ein Bericht verfasst und veröffentlicht werden.

7.3 Europarat

Die DSS hat im Berichtsjahr an der 44. und 45. 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 Leitlinien zum Datenschutz bei der Verarbeitung personenbezogener Daten zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung verabschiedet. Ausserdem hat er zwei Sets von Standardvertragsklauseln für grenzüberschreitende Datentransfers erlassen. Im Übrigen bestand die Hauptarbeit des Beratenden Ausschusses weiterhin in der Erarbeitung von Berichten, Positionspapieren u.ä. etwa zur Datenverarbeitung im Rahmen von Abstimmungen und Wahlen. 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. Die DSS unterstützte das Amt für Auswärtige Angelegenheiten im Berichtsjahr erneut beim Ratifikationsprozess des Änderungsprotokolls. Die formelle Ratifikation desselben durch Liechtenstein erfolgte am 17. Mai 2023 anlässlich des Gipfeltreffens des Europarats in Reykjavík. Insgesamt sind 38 Ratifikationen erforderlich, damit das Änderungsprotokoll bzw. die modernisierte Konvention 108+ in Kraft treten kann. Das Erreichen dieser Marke wird für 2024 erwartet. 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.

«Es ist wichtig, dass neben der Bewältigung neuer Herausforderungen auch bewährte Praktiken beibehalten werden.»

8. Schlussbemerkung und Ausblick

Die EU-Kommission hat eine breit angelegte Dateninitiative ins Leben gerufen, die eine Vielzahl neuer Gesetze umfasst. Bereits beschlossene Massnahmen wie der Data Governance Act, der Digital Services Act und der Digital Markets Act sind schon in Kraft getreten und wirksam. Weitere Gesetze wie der Data Act, der Artificial Intelligence Act und der European Health Data Space werden in naher Zukunft beschlossen werden oder Wirksamkeit erlangen. Auch Liechtenstein als EWR-Staat wird von diesen Neuerungen betroffen sein, wenngleich vermutlich in etwas geringerem Ausmass als in der EU. Für die DSS bedeutet dies zahlreiche neue Fragestellungen und Unterstützung der Ämter und Stellen, die für die nationale Umsetzung verantwortlich sein werden. Vor allem das Verhältnis zur DSGVO ist noch nicht restlos geklärt und erfordert noch einiges an Koordinierung.

Im Berichtsjahr wurde ausserdem erfolgreich ein Projekt gestartet, das bereits weit fortgeschritten ist: die Umstellung der Vorratsdatenspeicherung auf eine Anlassdatenspeicherung. Seit vielen Jahren hat die DSS Bedenken hinsichtlich der Eingriffe in die Privatsphäre der Bürgerinnen und Bürger durch die Vorratsdatenspeicherung geäussert. Die Bedenken der DSS hinsichtlich der Eingriffe in die Privatsphäre wurden durch die zunehmende Digitalisierung und die wachsende Menge an persönlichen Daten verstärkt. Die Umstellung auf eine Anlassdatenspeicherung stellt daher nicht nur eine rechtliche Anpassung dar, sondern auch einen wichtigen Schritt zur Stärkung des Datenschutzes in einer zunehmend digitalisierten Welt. Die DSS wird auch im Jahr 2024 ihre Expertise zur Verfügung stellen, um das Projekt erfolgreich abzuschliessen und zu finalisieren.

Es ist wichtig, dass neben der Bewältigung neuer Herausforderungen auch bewährte Praktiken beibehalten werden. Die langjährige Beratungstätigkeit der DSS hat sich als äusserst erfolgreich erwiesen und wird sowohl von öffentlichen als auch privaten Stellen sehr geschätzt und intensiv genutzt. Die DSS richtet ihre Aktivitäten eng an den tatsächlichen Bedürfnissen aus, um sicherzustellen, dass sie den Anforderungen der Verantwortlichen und betroffenen Personen gerecht wird und nicht an ihnen vorbeigeht. Aus diesem Grund wird die DSS auch im kommenden Jahr wieder offen für Anfragen und Vorschläge sein und sich bemühen, diesen so weit wie möglich nachzukommen.

Datenschutzstelle Fürstentum Liechtenstein
Städtle 38
Postfach 684
FL-9490 Vaduz

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