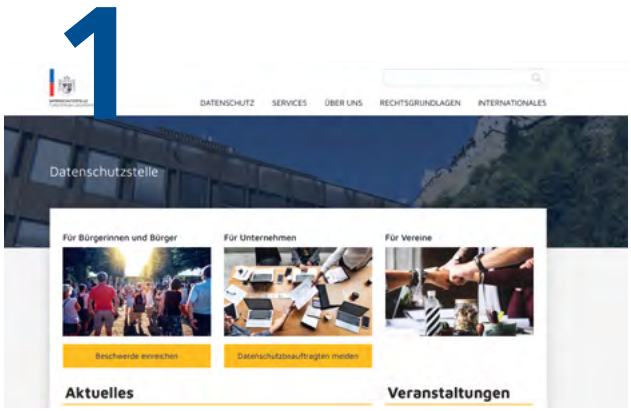
DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht Datenschutzstelle
Fürstentum Liechtenstein

Tätigkeitsbericht 2022

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

Der Tätigkeitsbericht 2021 endete mit dem folgenden Blick in die Zukunft: «Ein Ausblick auf das Jahr 2022 lässt vorsichtigen Optimismus aufkommen. Im Vergleich zum vergangenen Jahr scheint dieser Optimismus diesmal doch angebracht, die «neue Normalität» zumindest zu einem Teil wieder durch die «alte Normalität» zu ersetzen.»

Aus Sicht der Datenschutzschutzstelle (DSS) erfüllte sich der Wunsch nach Normalität im Berichtsjahr tatsächlich. Alle Veranstaltungen konnten wie in den Jahren vor der Covid-Pandemie gemäss Planung stattfinden. Auch die Themen der Anfragen waren wieder äusserst vielfältig und zahlreiche Projekte, die in den Unternehmen und öffentlichen Stellen während der Pandemie stillgestanden hatten, wurden wiederaufgenommen und gaben Anlass für zahlreiche herausfordernde Fragen zum Datenschutz. Im Rahmen dieser Beratungen konnten im Berichtsjahr auch wieder viele Besuche in Präsenz stattfinden, was die Kooperation für beide Seiten deutlich vereinfachte und zu einem regen Austausch Anlass gab.

Andererseits zeigten die im Berichtsjahr nach einer längeren Unterbrechung wieder durchgeführten amtswegigen Datenschutz-Überprüfungen, dass doch eine beträchtliche Zahl von Unternehmen den Datenschutz in den letzten Jahren etwas aus den Augen verloren bzw. diesen trotz der inzwischen mehrjährigen Geltung der DSGVO noch gar nicht auf ihrer Agenda hatte. Der Tätigkeitsbericht ist daher auch ein Appell an alle Verantwortlichen und Auftragsverarbeiter, sich mit dem Thema Datenschutz eingehend auseinanderzusetzen und das Beratungsangebot der DSS anzunehmen. Ein Prüfverfahren ist nicht nur für die DSS mit grossem Aufwand verbunden, sondern vor allem für die Verantwortlichen. Dieser wäre leichter mit einer präventiven Umsetzung der Datenschutz-Anforderungen unter Zuhilfenahme der Expertise der DSS zu bewältigen.

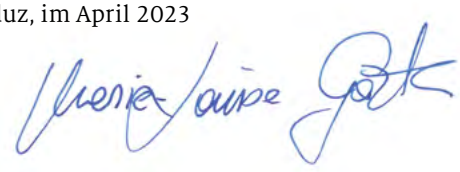
Im internationalen Umfeld stellten sich ebenfalls viele Herausforderungen. Sie ergaben sich vor allem im Zusammenhang mit den Tätigkeiten des Europäischen Datenschutzausschusses (EDSA) und der Umsetzung der Kooperation der Aufsichtsbehörden in grenzüberschreitenden Verfahren sowie der weiteren Präzisierung der Bestimmungen durch Leitlinien etc. Darüber hinaus sorgten auch die aktuellen Gesetzgebungspläne der EU zu den europäischen Digitalrechtsakten für zahlreiche Diskussionen in Bezug auf ihr Verhältnis zur DSGVO sowie zur künftigen Umsetzung in Liechtenstein. Letztere bringt vor allem die Frage

Dr. Marie-Louise Gächter, Leiterin Datenschutzstelle

mit sich, wo die Verantwortung für diese Umsetzung angesiedelt werden soll. Die DSS zeigt sich hier kooperativ und ist auch bereit, Verantwortung zu übernehmen, soweit das dafür erforderliche Personal zur Verfügung gestellt wird.

Im Berichtsjahr hat sich aufgrund der fortschreitenden Digitalisierung in allen Lebens- und Arbeitsbereichen, einschliesslich der Verarbeitung sensibler Daten, der Arbeitsaufwand in der DSS erneut erhöht. Diese Herausforderung konnte nur dank der motivierten und engagierten Mitarbeitenden der DSS bewältigt werden. Ich möchte an dieser Stelle meinen herzlichen Dank für ihren grossen Einsatz, ihre Fähigkeit, auch in schwierigen Situationen einen kühlen Kopf zu bewahren, und ihre Hilfsbereitschaft aussprechen. Ebenso gilt ein grosser Dank den behördlichen und betrieblichen Datenschutzbeauftragten, mit denen die DSS zusammenarbeiten darf, sowie den engagierten Bürgerinnen und Bürgern, die ihre Rechte wahrnehmen und die DSS auf Missstände aufmerksam machen.

Vaduz, im April 2023



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

1. Öffentlichkeitsarbeit

Insbesondere die schnell fortschreitende technische Entwicklung, aber auch die nach wie vor offenen Fragen und Unsicherheiten in Bezug auf den internationalen Datentransfer warfen im Berichtsjahr wieder zahlreiche Fragen auf. Zusätzlich zu den neuen Herausforderungen zeigten jedoch vor allem die amtswegigen Untersuchungen der DSS, dass viele Verantwortliche nach wie vor auch noch mit Grundsatzfragen beschäftigt sind und sich die Umsetzung der DSGVO in zahleichen Unternehmen noch in den Anfängen befindet. Insbesondere zeigen sich diese Lücken bei der Gestaltung der Internetseiten, deren Qualität in Liechtenstein aus Datenschutzsicht noch grossen Nachholbedarf aufweist. Folglich ist auch die Anzahl der Beschwerden in Bezug auf nicht datenschutzkonforme Internetseiten im Verhältnis zu anderen Beschwerdegründen recht hoch. 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.

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. Glücklicherweise mussten im Berichtsjahr nur mehr wenige Veranstaltungen aufgrund der Covid-19-Beschränkungen abgesagt oder auf kleine Kreise beschränkt werden. Den Grossteil der Veranstaltungen konnte die DSS wieder wie geplant durchführen.

1.1 Veranstaltungen

Nachdem der Datenschutztag, der wie üblich jedes Jahr Ende Januar stattfindet, auf Grund der Covid-19-Beschränkungen im Jahr 2021 ausfallen musste, gelang es, die Veranstaltung im Juni des Berichtsjahres nachzuholen. Unter dem Thema «Überwachungsstaat – Illusion oder Realität?» konnte die DSS zwei renommierte Referenten gewinnen. Kai Strittmatter, ein deutscher Journalist und Buchautor, schilderte eindrücklich seine persönlichen Erfahrungen mit dem Überwachungsstaat China. Im Anschluss gab Franz Steger-Künz vom Verfassungsschutz Tirol einen Einblick in die Möglichkeiten und Grenzen staatlicher Überwachung in Europa. In der anschliessenden Podiumsdiskussion nahm Bruno Gstöhl von der Landespolizei Liechtenstein Stellung zur Frage, wie sich Liechtenstein zu einer solch weitreichenden staatlichen Überwachung der Bürgerinnen und Bürger stellt. Die Vorträge und die Diskussion machten deutlich, wie erheblich die Unterschiede zwischen Europa und China sind und welch unterschiedlicher Status dem Schutz personenbezogener Daten zugewiesen wird. Während in Europa der einzelne Mensch und das Menschenrecht auf Privatsphäre bzw. auf Schutz personenbezogener Daten im Mittelpunkt der Frage der Verarbeitung von Daten steht, werden Daten in China so gut wie unbeschränkt dem Staat überlassen, der für gesellschaftliches Wohlergehen sowie soziale und nationale Sicherheit und Kontrolle sorgen soll.

Ebenfalls konnte im Herbst des Berichtsjahres wieder das Vernetzungstreffen für Datenschutzbeauftragte stattfinden. Der rege und kontinuierliche Austausch mit den Datenschutzbeauftragten nimmt 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 Datenschutzbeauftragten 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.

Auf Grund der bis ins Frühjahr 2022 andauernden Planungsunsicherheit, entschied die DSS, im Berichtsjahr auf die Durchführung von Workshops zu verzichten.

Gemäss Art. 15 Abs. 1 Bst. b DSG gehört es zu den Aufgaben der DSS «die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären, wobei spezifische Massnahmen für Kinder besondere Beachtung finden». In der Vergangenheit konzentrierte sich die DSS mit ihrer Öffentlichkeitsarbeit schwergewichtig auf Kinder und Jugendliche bzw. deren Eltern, nicht zuletzt, weil diese im genannten Artikel speziell er-

wähnt werden. Diesen Ansatz verfolgte die DSS auch im Berichtsjahr weiter.

Am 29. September führte die DSS das erste Mal einen Anlass im Rahmen der neuen Reihe «Datenschutz goes Cinema» durch. In Kooperation mit dem Skino in Schaan zeigte sie den Kino-Dokumentarfilm «Hinter den Schlagzeilen». Anschliessend gab es mit dem Regisseur sowie weiteren hochrangigen Gästen aus Journalismus und Jurisdiktion eine Podiumsdiskussion zur Rolle von Datenschutz und Privatsphäre in den Medien bzw. zur Frage, was Medienschaffende bei ihren Recherchen alles dürfen oder wo auch sie entsprechende Grenzen zu achten haben. Der Anlass und das neue Format stiessen bei der Bevölkerung auf grossen Anklang, weswegen die Veranstaltungsreihe in den Folgejahren 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 wurde wieder schwerpunktmässig mit den beiden Universitäten in Liechtenstein zusammengearbeitet und gemeinsame Veranstaltungen angeboten.

Am 30. November fand an der Privaten Universität zum vierten Mal in Folge eine ganztägige Weiterbildungsveranstaltung im Datenschutz zum Thema «Von neuen Stolpersteinen und wie sie vermieden werden» statt. Der Vortrag der DSS im Rahmen der im Gemeindesaal Triesen durchgeführten Veranstaltung befasste sich mit dem Thema «EU-U.S. Data Privacy Framework und die Verwendung von US-Cloudsystemen». Das EU-U.S. Data Privacy Framework soll die Nachfolge des EU-U.S. Privacy Shields antreten und somit für die USA einen neuerlichen Angemessenheitsbeschluss gewährleisten. Zum Zeitpunkt der Veranstaltung bestanden noch zahlreiche offene Fragen im Hinblick auf die Verhandlungen zwischen den USA und der EU. Der Vortrag beleuchtete diese Unsicherheiten und die Wahrscheinlichkeit, ob der Angemessenheitsbeschluss auch tatsächlich bis Sommer 2023 zustande kommen wird.

Der zweite Schwerpunkt des Vortrags widmete sich der Verwendung von US-Cloudsystemen, die an Beliebtheit stark zunehmen und auch häufig Gegenstand der Beratungstätigkeit der DSS sind. Ein Vorteil einer Cloud-Lösung ist beispielsweise ihre Skalierbarkeit, die es Unternehmen ermöglicht, je nach Bedarf schnell und einfach ihre IT-Infrastruktur zu erweitern oder zu reduzieren. Cloud-Lösungen ermöglichen es zudem Benutzern, von überall auf Daten und Anwendungen zuzugreifen, solange sie eine Internetverbindung haben. Dies bedeutet, dass Benutzer nicht mehr an einen bestimmten Ort gebunden sind und dass die Zusammenarbeit zwischen Teammitgliedern, die an verschiedenen Standorten arbeiten, erleichtert wird. Auch bieten Cloud-Lösungen oft höhere Sicherheitsstandards als lokale IT-Infrastrukturen, da sie in der Regel mit fortschrittlichen Sicherheitsfunktionen wie Verschlüsselung, Zugriffskontrolle und regelmässigen Backups ausgestattet sind. Nichtsdestotrotz benötigt die Entscheidung, eine Cloud-Lösung einzusetzen, Zeit und eine sorgfältige Auseinandersetzung mit den angebotenen Möglichkeiten. Dies sollte ebenso wenig unterschätzt werden wie eine genaue Ausgestaltung des Auftragsverarbeitungsvertrages. Hier ist es insbesondere wichtig, dass der Auftragsverarbeiter vertraglich festlegt, welche konkreten technischen und organisatorischen Massnahmen er zur Gewährleistung der Datensicherheit zur Verfügung stellt.

Soweit Cloud-Systeme von US-Anbietern verwendet werden, ist zudem darauf zu achten, dass die Vorgaben der DSGVO betreffend internationalen Datentransfer eingehalten werden. Solange der Angemessenheitsbeschluss für die USA noch ausstehend ist, gestaltet sich die Einhaltung der geforderten Garantien als schwierig, wenn sich der Serverstandort in den USA befindet. Wenn er hingegen im EWR ist, relativiert sich die Frage etwas, allerdings ist auch die Anwendung des amerikanischen CLOUD-Acts nicht zu unterschätzen und sollte bei der Entscheidung mitberücksichtigt werden. Nicht zuletzt hängen diese Fragen vom Zweck ab, zu dem auf eine Cloud-Lösung zurückgegriffen wird, sowie der Sensibilität der verarbeiteten personenbezogenen Daten.

Auf Einladung der Universität Liechtenstein übernahm die DSS mehrere Lektionen im Rahmen des Zertifikationsstudiengangs «Digital Legal Officer» im Dezember. Ein erster Teil befasste sich mit der Frage der Datensicherheit aus rechtlicher Perspektive, der Datenschutz-Folgenabschätzung, Meldungen einer Datenschutzverletzung unter Art. 33 DSGVO aus Sicht der Aufsichtsbehörde sowie dem internationalen Datentransfer. Der zweite Teil widmete sich technischen Aspekten bezüglich Datensicherheit, Data Protection by Design and by Default sowie Cookie-Management. Es wurden sowohl grundlegende Konzepte der Datensicherheit als auch die praktische Umsetzung von technischen und organisatorischen Massnahmen unter Berücksichtigung des aktuellen Standes der Technik anhand von realen Fallbeispielen erläutert. Neben

dem Prinzip von Data Protection by Design and by Default wurde insbesondere auf die technischen Grundlagen von Cookies, ihre Zwecke und ihre Bedeutung für den Datenschutz speziell in Bezug auf Third-Party Cookies und Cookie-Banner, eingegangen.

1.2.2 Kooperation mit dem Schulamt

Das Schulamt gelangte im Berichtsjahr mit der Anfrage an die DSS, für Lehrpersonen einen Workshop zur Gestaltung von Internetseiten anzubieten. Die DSS kam dieser Bitte gerne nach. Damit möglichst viele Lehrpersonen teilnehmen konnten, wurde der Workshop im März online durchgeführt. Neben den datenschutzrechtlichen Grundlagen wurde der Schwerpunkt vor allem auf technische Aspekte, die es bei der Ausgestaltung einer Internetseite zu beachten gilt, gelegt. Um ein tieferes Verständnis für die heutigen Herausforderungen im Zusammenhang mit Internetseiten vermitteln zu können, wurde ein kurzer geschichtlicher Abriss bezüglich der Entwicklung des Internets, und insbesondere der Entstehung von Webseiten, dargestellt. Oft angesprochene Themen, wie beispielsweise Cookies und Cookie-Banner, Einbettung von Skripten, die in der Regel einen Datentransfer (u.a. auch in Drittländer) mit sich bringen, als auch konkrete Werkzeuge zur Analyse von Internetseiten, wurden kritisch auf ihre Datenschutzkonformität beleuchtet.

1.2.3 Fachgruppe Medienkompetenz LIHGA 2022

Im Rahmen der Beteiligung der DSS bei der Fachgruppe Medienkompetenz war ein Schwerpunkt die Teilnahme an der LIHGA unter dem Motto «Fake News». Am Stand der Fachgruppe konnte sich das Publikum rund um das Thema «Fake News» informieren. Um möglichst viele Personen zu begeistern, hatte die Fachgruppe zudem zwei Stationen, bei denen sich die Interessenten aktiv beteiligen konnten, eingerichtet. Neben einem Quiz, bei dem zwischen «fake» und realen Bildern unterschieden werden musste, bestand auch die Möglichkeit, «fake» Bilder mit Hilfe eines grünen Hintergrunds selbst zu produzieren. Zudem wurden «Fake News»-Plakate von Schülerinnen und Schülern der Realschule Balzers gestaltet, die für eine interessante Diskussionsgrundlage sorgten.

1.2.4 LLV Kurs Smartphone und Internet

Wie schon im Jahr 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 Hintergründe und Grundsätze zum Schutz des informationellen Selbstbestimmungsrechtes als auch 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.

1.2.5 Weitere Vorträge

Zusätzlich zu den erwähnten Veranstaltungen nahmen Mitarbeitende der DSS an 18 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) die DSS zu einer Veranstaltung in Zürich für betriebliche Datenschutzexperten ein. Themen der Diskussion waren neben dem internationalen Datentransfer vor allem die neue Rechtsprechung des Europäischen Gerichtshofs (EuGH) zu besonderen Kategorien personenbezogener Daten (Urteil in der Rechtsache C-184/20 vom 1. August 2022) sowie die Frage, ob es tatsächlich ausser Zweifel steht, dass man die IP-Adresse als personenbezogenes Datum qualifizieren kann. Ein weiteres Thema war die zweckwidrige Geltendmachung von Betroffenenrechten. 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.

Des Weiteren war die DSS im Berichtsjahr mit je einem Beitrag am «Privacy Symposium» in Venedig und am «Forum Privatheit 2022: Daten-Fairness in einer globalisierten Welt – Grundrechtsschutz und Wettbewerb für eine internationale Data Governance» in Berlin vertreten.

Schliesslich wirkte die DSS auch bei verschiedenen, von Unternehmen ausgerichteten Veranstaltungen mit. Im Besonderen leistete die DSS im Berichts-

jahr wieder Beiträge bei Veranstaltungen dieser Unternehmen für ihre Lernenden. 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 Mitarbeiterschulungen

Die DSS wurde auch im Berichtsjahr wieder von liechtensteinischen Firmen für Mitarbeiterschulungen in die Unternehmen eingeladen. Die DSS konnte so beispielsweise erneut eine Präsentation mit anschliessender Fragerunde für eine Vermögensverwaltungsfirma durchführen. Dabei konnten nicht nur Fragen zu Branchen-spezifischen Themen, sondern auch zu vielen weiteren Datenschutzthemen von der DSS beantwortet werden.

Solche gezielten Mitarbeiterschulungen stellen für die DSS ein probates Mittel dar, im Sinne der Beratung und Sensibilisierung direkt bei den Verantwortlichen tätig zu werden und datenschutzrechtliche Themen praxisnah und speziell auf eine Branche bezogen zu erklären. Durch die gleichzeitig aufkommenden und beantworteten Fragen entsteht so auch ein gewisses Feedback und direkter Dialog mit der DSS, welcher der DSS hilft, bei ihrer aufklärenden und informierenden Arbeit zielgerichtete Prioritäten zu setzen.

1.3 Internetseite

Zwei weitere wesentliche Elemente der Öffentlichkeitsarbeit der DSS sind der Internetauftritt sowie der circa zweimal monatlich 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 zum Thema Google Analytics, zur Datenrichtigkeit und Datenqualität, zur Zweckänderung, zur Nutzung von Smartphones an der Fussball-WM in Katar, zu IT-Sicherheitsvorfällen (Cybersicherheit), zu den neuen Standardvertragsklauseln für internationale Datentransfers (SCC) sowie zum neuen EU-U.S. Data Privacy Framework. 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 erneut bei folgenden Beiträgen verzeichnet: Berechtigtes Interesse, Informationspflicht nach Art. 13 und 14 DSGVO, kleines Konzernprivileg, Verzeichnis der Verarbeitungstätigkeiten und Datenschutzerklärung für Internetseiten.

1.4 Newsletter

Im Berichtsjahr wurde das Newsletter-Tool der LLV erneuert. Dies bedingte, dass sich sämtliche Abonnentinnen und Abonnenten mittels «Double Opt-in»-Verfahren neu für den Newsletter der DSS anmelden mussten. Ende 2022 hatten 821 Personen den Newsletter der DSS neu abonniert und das Interesse daran ist somit nach wie vor ungebrochen. Diese Abonnentenzahl entspricht zwar einem Minus von 30% gegenüber dem Vorjahr, doch erlaubte die Erneuerung des Newsletter-Tools auch eine Bereinigung des Verteilers, mit der viele inaktive E-Mail-Adressen aussortiert werden konnten. Nachdem die Zeitspanne für die Umstellung mehrere Wochen in Anspruch nahm und während dieser Zeit kein Newsletter-Versand möglich war, ist die Zahl der im Berichtsjahr versandten Newsletter mit 17 etwas geringer als üblich. Die drei meistgelesenen Newsletter 2022 waren die Information zu Google Analytics und dem Datenschutz, das Update des Fragebogens zur DSGVO-Umsetzung (Selbstevaluation), sowie die Aktualisierung der Liste der gesetzlichen Lösch- und Aufbewahrungsfristen.

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. Weil 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

Auch im Berichtsjahr war der Datenschutz wieder prominent in den liechtensteinischen Medien vertreten. Themen der über 40 Berichte in den Printmedien waren das elektronische Gesundheitsdossier, der Austausch von Casino-Sperrlisten mit der Schweiz, ein vermutliches Leck bei einem Corona-Testcenter, die Erhebung des Kilometerstandes von geprüften Fahrzeugen durch das Amt für Strassenverkehr sowie der Datenschutz im Schulbereich. Einige dieser Themen beschäftigten die DSS auch im Rahmen von Beratungen oder Beschwerden gemäss Art. 77 DSGVO.

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 Berufswegen weniger Berührungspunkte mit dem Datenschutz haben.

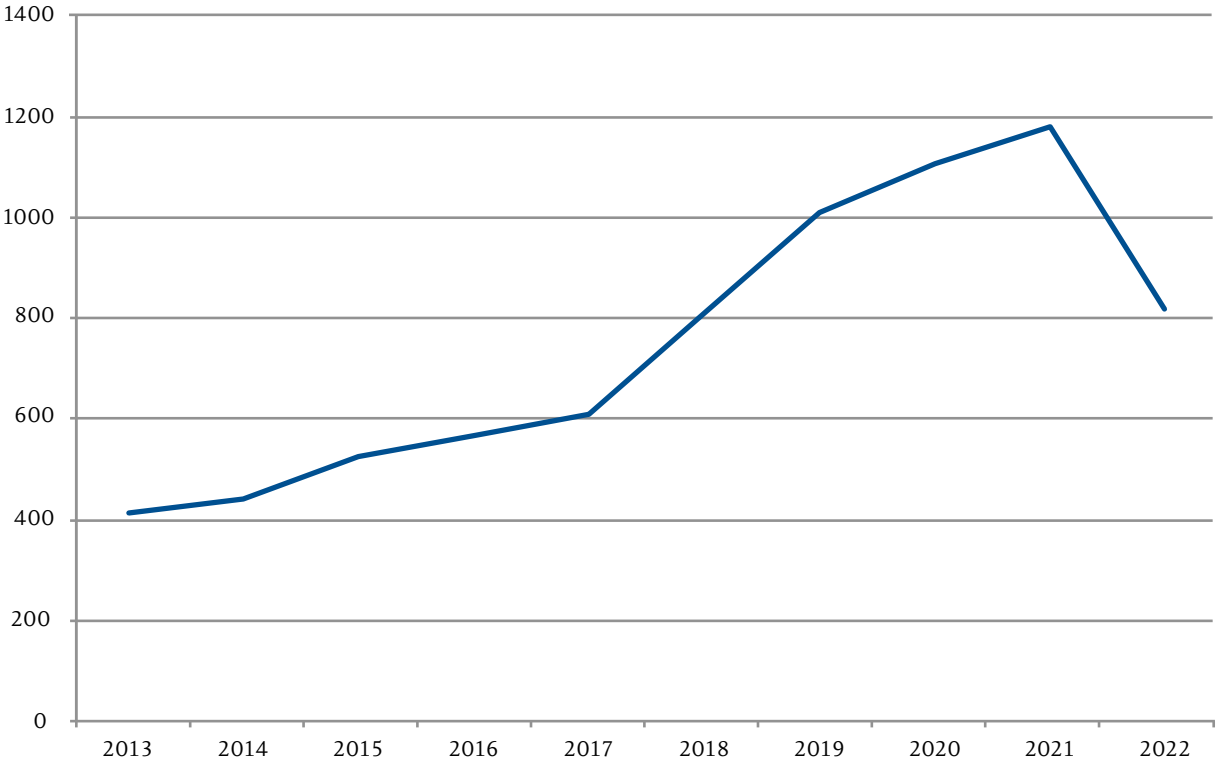


Abbildung 1: Entwicklung Newsletter-Abonnentinnen und Abonnenten

«Privatpersonen machten 9,4 % der Fragestellenden aus und zeigten damit erneut grosses Interesse am Datenschutz.»

2. Beratung zu konkreten Anfragen

2.1 Allgemeines

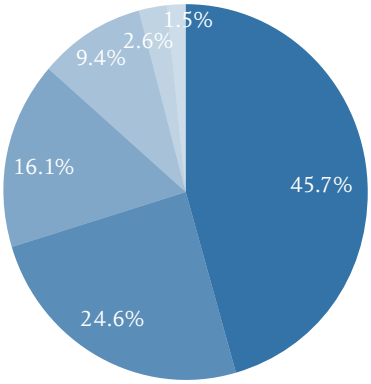
Im Berichtsjahr verzeichnete die DSS 1'503 Anfragen von öffentlichen und privaten Institutionen sowie Privatpersonen. Im Vergleich zu den im Vorjahr beantworteten 1'284 Anfragen bedeutet dies einen Zuwachs um 17%. Bereits seit zwei Jahren war zudem eine deutliche Steigerung der Komplexität der Anfragen zu verzeichnen, welche im Berichtsjahr ebenfalls klar anhielt. Ebenso zeigte sich, dass der technische Fortschritt zahlreiche neue und herausfordernde Fragen aufwirft, ob und inwieweit die jeweiligen technischen Systeme die Datenschutzanforderungen erfüllen können. Die erneut zahlreiche und umfangreiche Beratung der DSS zum Einsatz von Videoüberwachungsanlagen durch Private oder Unternehmen, welche vertiefte Kenntnisse im rechtlichen wie auch technischen Bereich verlangte, sei dabei im Besonderen genannt. Nach wie vor bestanden weiterhin grosse Unsicherheiten in Bezug auf das «Schrems II»-Urteil des EuGH vom 16. Juli 2020 und vor allem betreffend die nachfolgenden Beschwerden von Max Schrems bzw. seiner Datenschutzorganisation «noyb» zur Frage der Zulässigkeit von Google Analytics sowie der Verarbeitung von personenbezogenen Daten mittels Facebook Connect. Auch Fragen zu Cookies sowie der rechtskonformen Ausgestaltung von Cookie-Bannern kamen sehr häufig vor.

In Bezug auf die Herkunft der Fragesteller ist festzuhalten, dass diese dem Trend der letzten Jahre folgend erneut zu einem grossen Teil aus der Privatwirtschaft stammten (45.7%), wobei sich der Anteil im Berichtsjahr sogar noch deutlich vergrösserte. Rund ein Drittel dieser Anfragen wiederum kam aus der Finanzindustrie. An zweiter und dritter Stelle folgten internationale Anfragen (24.6%) sowie die Landesverwaltung und die Gemeinden (16.1%). Privatpersonen machten 9.4% der Fragesteller aus, die damit erneut grosses Interesse am Datenschutz zeigten. Die Anfragen von Vereinen und Stiftungen (2.6%) sowie von den Medien (1.5%) waren im Berichtsjahr rückläufig.

Beratungsanfragen konnten telefonisch, schriftlich – insbesondere mittels E-Mail – oder auch in einem persönlichen Gespräch bei der DSS eingebracht werden. Von den 1'503 Anfragen wurden im Berichtsjahr 144 telefonisch gestellt und beantwortet. Sie stammten von 123 Anrufern, was einem neuerlichen leichten Rückgang im Vergleich zu den Vorjahren entspricht (2021: 156 Anrufer; 2020: 214 Anrufer). Die Begründung liegt auch hier in der bereits erwähnten Zunahme der Komplexität der Fragestellungen, wodurch einfache telefonische Anfragen und Auskünfte stark abnehmen.

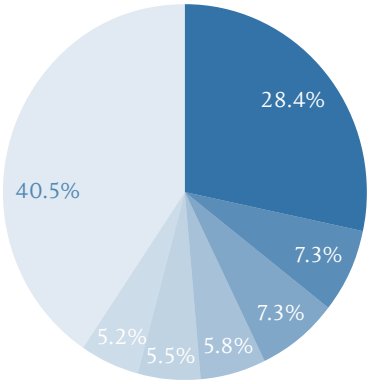
Ganz allgemein stellte sich auch im Berichtsjahr wieder die Frage, ob und in welchem Ausmass eine

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

Datenschutz-Aufsichtsbehörde überhaupt beratend tätig sein sollte bzw. ob Aufsicht durch Beratung überhaupt im Sinne der DSGVO ist. Die DSS blieb jedoch 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».

Nichtsdestotrotz zeigte sich gerade im Berichtsjahr sehr deutlich, dass das Beratungsangebot bedauerlicherweise von vielen nicht wahrgenommen wird. Die amtswegigen Datenschutz-Überprüfungen ergaben, dass nach wie vor zahlreiche Unternehmen wenig bis gar keine Sensibilität in Bezug auf den Schutz personenbezogener Daten aufweisen. Obwohl die DSS jede Gelegenheit nützt, auf ihr kostenloses Beratungsangebot hinzuweisen, bleibt es natürlich den Unternehmen überlassen, dieses auch anzunehmen und einzufordern. Die DSS möchte jedoch im Folgejahr wieder neue Gelegenheiten suchen, um noch mehr auf das Beratungsangebot aufmerksam zu machen und um auf diese Weise das schlechte Abschneiden zahlreicher Unternehmen bei den Datenschutz-Überprüfungen zu verhindern.

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

2.2 Videoüberwachung und Veröffentlichung von Bildmaterial

Mit Inkrafttreten des DSG erfuhr die Videoüberwachung öffentlich zugänglicher Räume in Art. 5 eine neue gesetzliche Regelung. Wie die DSS in ihren letzten Tätigkeitsberichten erläuterte, nahmen in Folge dessen die Anfragen zur Videoüberwachung stark zu. Dieser Trend hielt auch 2022 weiter an. 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.

Schon in den vergangenen Tätigkeitsberichten informierte die DSS 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

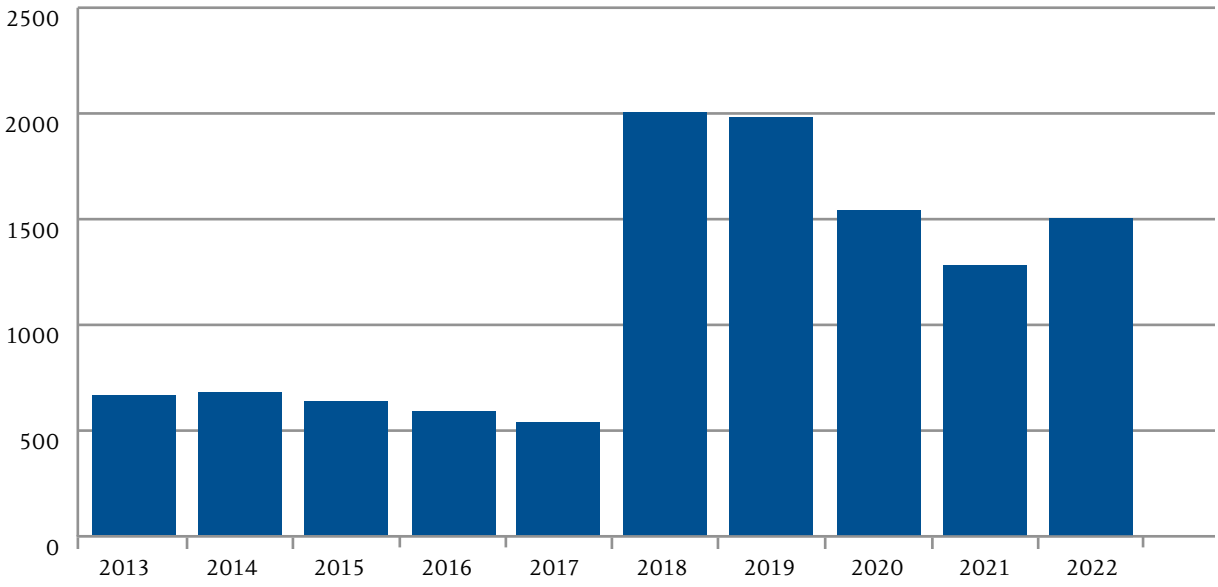


Abbildung 2: Anzahl der Anfragen pro Jahr

nicht nachgelassen und beschäftigt die DSS nach wie vor intensiv. So sind im Berichtsjahr 8 Drohnenflüge mit Kameras und 22 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 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. Dies ist etwa im Fall einer Videoüberwachung geschehen, welche eine Gemeinde in einer Freizeitanlage betreibt. Die Details dazu werden im Kapitel Aufsicht beschrieben.

Neben der Prüfung von eingegangen 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 diesem Zusammenhang war die DSS bei Videoüberwachungen in Geschäften und deren Ausstellungsräumen beratend tätig. Hierbei stellt sich insbesondere die Frage einer potentiellen Überwachung der Mitarbeitenden. Zu deren Schutz ist es unerlässlich, die Videokameras so zu positionieren und den Bildausschnitt so zu wählen, dass die Mitarbeitenden maximal für kurze Zeitspannen miterfasst werden. Mitarbeitende sind zudem über die Positionen und Einstellungen der Kameras detailliert zu informieren, damit sie den überwachten Bereich kennen und nach Möglichkeit ein längeres Verweilen im Aufnahmebereich vermeiden können.

Eine weitere umfassende Beratung erfolgte in Bezug auf einen Restaurantbetrieb. Videoüberwachungen, welche Sitzbereiche in Restaurants, Bars und Cafés erfassen, sind datenschutzrechtlich sehr kritisch zu sehen und selten zulässig. Vor dem Einsatz von Videokameras hat stets eine umfassende Güter- und Interessenabwägung unter Beachtung der rechtlich geschützten Positionen sämtlicher Beteiligten und unter Würdigung der jeweiligen Umstände zu erfolgen. Es ist vor allem zu berücksichtigen, dass die Gäste das Restaurant als Rückzugsraum aufsuchen, wo sie sich ungestört und unbeobachtet unterhalten wollen und sich in den meisten Fällen auch länger aufhalten. Ausserdem ist zu berücksichtigen, dass gegebenenfalls durch die Überwachung des Gastraumes auch Mitarbeitende erfasst werden können. Hinsichtlich der Mitarbeiterüberwachung ist ein besonders strenger Massstab anzulegen, wie bereits oben ausgeführt wurde. Folglich überwiegt das berechtigte Interesse an einer Videoüberwachung des Betreibers nur selten die berechtigten Interessen an einer unbeobachteten Ausübung einer sozialen, gesellschaftlichen und kulturellen Freizeitaktivität. Videoüberwachungen in Restaurationsbetrieben können daher grundsätzlich lediglich im Kassenbereich (etwa bei Take-Away Betrieben), im Lieferantenbereich und bei Mitarbeitereingängen und/oder ausserhalb der Öffnungszeiten zulässig sein. Aber auch dafür bedarf es einer sorgfältigen Einzelfallabwägung.

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.

Auch im Bereich der staatlichen Videoüberwachung war die DSS beratend tätig. Neben der projektierten Videoüberwachung der Tiefgarage des Landtagsgebäudes und des Peter-Kaiser-Platzes beriet die DSS auch eine Gemeinde bezüglich einer Videoüberwachung von Fahrradständern und einer Bushaltestelle. Die DSS hat dabei Wert daraufgelegt, dass von den Kameras keine Bereiche erfasst werden, welche für den längeren Aufenthalt und somit zur Ausübung des Freizeitverhaltens von Personen ausgelegt sind. Beispielsweise wurden die Sitzbank im Wartebereich der Bushaltestelle ebenso wie die Sitzgelegenheiten auf der angrenzenden Grünfläche vom Erfassungsbereich der Kamera ausgenommen.

Weiters wurde 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 hinzugezogen. Nachdem erste Besprechungen dazu bereits im Vorjahr stattgefunden hatten, wurde die Videoüberwachung an den diversen Standorten im Berichtsjahr installiert und in Betrieb

genommen. Die Anforderungen der DSS wurden dabei vollumfänglich berücksichtigt. So werden die Videoüberwachungen beim Lindaplatz, beim SAL sowie bei der Kreuzung nach Nendeln lediglich anlassbezogen in Betrieb genommen. Die Interessenabwägung hat hier ergeben, dass das berechtigte Interesse der Bevölkerung, vom Staat nicht über eine längere Zeitdauer beobachtet zu werden, gegenüber dem Interesse an einer umfassenden und anlasslosen Überwachung überwiegt. In den anderen Bereichen hingegen ist die Videoüberwachung aufgrund einer erhöhten Kriminalitätsrate zulässig. Auch hier erfolgte jedoch eine Eingrenzung des Aufnahmeradius auf die unbedingt erforderlichen Bereiche. Die DSS wurde Ende des Berichtsjahrs über die erfolgte Implementierung informiert. Eine angemessene Kenntlichmachung der Videoüberwachung und die Information über die wesentlichen Eckpunkte der Videoüberwachung sowie weitergehende spezifische Information gemäss Art. 13 DSGVO auf der Internetseite der Landespolizei sind allerdings noch ausstehend und werden von der DSS im Folgejahr einer abschliessenden Kontrolle unterzogen. In Bezug auf die Informationspflicht der Landespolizei gegenüber der Bevölkerung ist essentiell, dass diese so umgesetzt wird, dass klar erkennbar ist, wann und wo eine Videoüberwachung erfolgt. Die Grund-Information ist überdies vor Ort so anzubringen, dass diese vor Betreten des überwachten Bereichs erkennbar ist und es Passanten erlaubt, dem überwachten Bereich auszuweichen.

Auch wenn keine öffentlich zugänglichen Bereiche erfasst werden und somit keine Meldung bei der DSS erforderlich ist, steht die DSS den Verantwortlichen beratend zur Seite. Dies war im Berichtsjahr beispielsweise der Fall bei einem geplanten Projekt zur Verkehrsdatenerfassung mittels Videoüberwachung sowie einer Videoüberwachung zur besseren Planung von Schneeräumungseinsätzen. Beide Videoüberwachungen erfassen zwar öffentlich zugängliche Räume, doch sind zur Zweckerreichung eigentlich gar keine personenbezogenen Daten notwendig. Folglich konnten die Videokameras so eingestellt werden, dass weder Personen noch Fahrzeuge (Nummernschilder) auf den Aufnahmen identifizierbar sind. Die Videoüberwachungen sind somit nicht vom Anwendungsbereich der DSGVO und des DSG erfasst und unterliegen deshalb auch nicht der Meldepflicht.

Immer grösserer Beliebtheit erfreuen sich ausserdem Kameras, die den Fortschritt eines Bauprojektes dokumentieren. Die DSS wurde in diesem Zusammenhang mehrfach beratend tätig. Auch bei Kameras zum Festhalten des Baufortschritts ist es zentral, dass diese so ausgestaltet sind, dass keine personenbezogenen Daten erfasst werden.

Dem Trend der Vorjahre folgend nahmen auch Videoüberwachungen im privaten familiären Bereich erneut zu und haben die DSS reichlich beschäftigt. Beratend hat sich die DSS mit Videoüberwachungen von Einfahrten und Vorplätzen zu Einfamilienhäusern befasst, aber auch mit der Überwachung von privaten Garagenparkplätzen von Mehrfamilienhäusern. Diese Fälle können grundsätzlich datenschutzkonform ausgestaltet werden. Wesentlich ist, dass keine öffentlich zugänglichen Bereiche oder Nachbargrundstücke erfasst werden. Als grundsätzlich unzulässig beurteilte die DSS hingegen eine Videoüberwachung in einem Lift eines Mehrfamilienhauses. Diese würde uneingeschränkt und anlasslos das Kommen und Gehen aller Eigentümer:innen, Mieter:innen wie auch von Besucher:innen erfassen und somit einen ungerechtfertigten Eingriff in deren Privatsphäre darstellen.

2.3 Verbindliche interne Datenschutzvorschriften

Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules; BCR) sind eine Möglichkeit gemäss 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.

Schon vor der DSGVO wurde das Konzept der BCR ausgearbeitet 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 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 Diskussionspunkte von allen europäischen Behörden abschliessend behandelt werden. Nach einem ersten zweitägigen Workshop der Arbeitsgruppe zu BCR 2019 in Oslo

fand im Berichtsjahr vorgängig zur Spring Conference eine Wiederauflage statt. In diesen Workshops geht es insbesondere darum, den Austausch und die einheitliche Anwendung und Durchsetzung der rechtlichen Vorgaben in Zusammenhang mit BCR zu fördern wie auch neue Mitarbeitende der verschiedenen Datenschutzbehörden in das Thema einzuführen. Dabei werden Beispiele, Probleme und Fragestellungen aus dem Erfahrungsschatz der verschiedenen Behörden vorgestellt und kollektiv erörtert und gemeinsame Lösungen und Vorgehensweisen abgesprochen. Zum Teil finden diese dann auch Eingang in die vom EDSA überarbeiteten Leitlinien zu den BCRs.

Ein schon länger aktuelles und viel diskutiertes Thema der Behörden 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 der federführenden Behörde und der zwei «Co-Reviewer» zeitlich parallel verlaufen können. Diese Schritte wurden bisher nacheinander geführt. Durch die Parallelität verspricht man sich nicht nur Zeitersparnisse, ohne die Überprüfungsqualität einzuschränken, sondern auch einen besseren Austausch bezüglich offener Fragen zwischen den überprüfenden Behörden.

Wie in den vergangenen Tätigkeitsberichten bereits erläutert, agiert die DSS seit 2019 als federführende Aufsichtsbehörde in einem Genehmigungsverfahren für BCR eines weltweit tätigen, liechtensteinischen Unternehmens. Nachdem die BCR finalisiert wurden und von den europäischen Datenschutzbehörden kein Widerspruch bzw. keine weiteren Kommentare mehr eingingen, erstellte die DSS einen Entscheidungsentwurf für die Genehmigung der BCR und übermittelte diesen an den EDSA. Nach positiver Stellungnahme des EDSA konnte die DSS das BCR-Verfahren im Herbst des Berichtsjahres mit einer entsprechenden Verfügung abschliessen. Das betreffende Unternehmen kann nun seinen internationalen Datentransfer im Rahmen der Anwendbarkeit und allfälliger zusätzlicher Massnahmen auf die BCR stützen. Zu den durch die BCR auferlegten Pflichten gehören etwa regelmässige Informationspflichten betreffend Änderungen und Aktualisierungen der BCR.

Wie im letztjährigen Tätigkeitsbericht bereits angekündigt, hatte ein weiteres, weltweit tätiges Unternehmen aus Liechtenstein Interesse an der Ausarbeitung von BCR bekundet. Zu Beginn des Berichtsjahres wurde der formelle Antrag eingereicht und die DSS als federführende Aufsichtsbehörde bestätigt. Die BCR konnten in der Folge dank einer effizienten und kooperativen Zusammenarbeit im Berichtsjahr erarbeitet werden. In diesem Verfahren wurde unter anderem auch von der oben erläuterten Möglichkeit Gebrauch gemacht und die beiden Co-Reviewer (Luxemburg und Deutschland (Baden-Württemberg)) bereits frühzeitig mit eingebunden. Ebenso fanden die Neuerungen der EDSA-Leitlinien bereits Eingang in die BCR, sodass nach der formellen Annahme der revidierten Leitlinien keine umfassende Überarbeitung nötig wurde.

Im Berichtsjahr hat erneut ein liechtensteinisches Unternehmen Interesse an der Ausarbeitung von BCR bekundet und es wurde bereits mit dem Prozess begonnen.

2.4 Auswahl konkreter rechtlicher Anfragen

Elektronischer Versand einer Rechnungskopie von einer ärztlichen Behandlung

Die Zusendung der Rechnung ist eine gesetzliche Verpflichtung. Grundsätzlich darf ein Arzt selbst entscheiden, ob er seinen Patienten die Rechnung für eine Behandlung per Briefpost oder per E-Mail zukommen lässt, wenn für beide Wege adäquate Sicherheitsstandards eingehalten werden. Welcher Weg dafür gewählt wird, hängt nicht von der Einwilligung ab, ausser dass natürlich die Bekanntgabe der E-Mail-Adresse erfolgen muss. Wichtig ist vor allem die Frage, ob der E-Mail-Versand den technisch geforderten Standards entspricht. Solange es sich somit um einen sicheren, dem Risiko der Gesundheitsdaten angemessenen Übermittlungsweg handelt, ist keine spezielle (zusätzliche) Einwilligung im Sinne des Art. 6 Abs. 1 Bst. a i.V.m. Art. 7 DSGVO erforderlich.

Testfahrten zu Kartierungszwecken

Im Berichtsjahr stellten mehrere ausländische Unternehmen die Frage an die DSS, unter welchen Voraussetzungen es zulässig ist, Kamerafahrten auf öffentlichen Strassen in Liechtenstein durchzuführen, die entweder dem Zweck der Erstellung von Karten dienen oder der automatisierten Erkennung von Strassenverkehrszeichen.

Für die Aufnahmen der Bilder (auf denen natürliche Personen nicht im Fokus stehen, aber in vielen Fällen doch identifizierbar sein können) dürfen sich die jeweiligen Unternehmen auf ihr berechtigtes wirtschaftliches Interesse nach Art. 6 Abs. 1 Bst. f DSGVO stützen. Vor der Veröffentlichung der Bilder (etwa in einem Fall im Rahmen des Apple «Look Around Features») müssen jedoch sämtliche Gesichter und Nummernschilder von den zufällig aufgenommenen Passanten und Fahrzeugen in den Bildern verpixelt

(unkenntlich gemacht) werden. Es dürfen zudem nur von der Strasse aus einsehbare Bereiche von Grundstücken aufgenommen und veröffentlicht werden.

Darüber hinaus muss betroffenen Personen die Möglichkeit gegeben werden, dieser Verarbeitung gemäss Art. 21 DSGVO jederzeit zu widersprechen und (so noch nicht geschehen) ein Verpixeln ihres Gesichts, Nummernschilds oder ihrer Hausfassade zu verlangen. Dies entspricht einer Löschung der personenbezogenen Daten. Das Verpixeln geschieht ausserdem auf den Rohdaten der Bilder, womit auch ein Verpixeln in künftigen Darstellungen gewährleistet ist. Idealerweise werden die Aufnahmedaten zudem bereits im Fahrzeug verschlüsselt, bevor sie an die Rechenzentren des Unternehmens geschickt werden.

Datenverarbeitung durch ein Maklerbüro

Im Rahmen der Tätigkeit eines Maklerbüros stellte sich die folgende Frage: Ein Immobilienmakler hat im Normalfall zwölf Monate Zeit, um ein Objekt zu vermarkten. Der Eigentümer möchte während dieser Zeit und auch nach Ablauf der Zeit bzw. Beendigung des Vertrages wissen, welche Interessenten den Makler kontaktiert haben. Grund ist, dass er die Maklergebühr bezahlen müsste, wenn sich eine Person, die sich ohne zu kaufen oder zu mieten beim Makler gemeldet hat, nun den Eigentümer direkt kontaktiert und es zu einem Kauf/Miete kommt. Aus Sicht der DSS ist es möglich, diese Information (entsprechend dem Grundsatz der Datenminimierung nur der Name) herauszugeben, gestützt auf Art. 6 Abs. 1 Bst. b DSGVO, wenn die Weitergabe während der Phase vorvertraglicher Massnahmen zwischen Makler und Interessenten stattfindet, oder auf Bst. f, wenn der Vertrag nicht zustande gekommen ist.

Offenlegung Protokolle Eigentümergemeinschaft an Kaufinteressenten

Eine Person möchte eine Wohnung in einem Mehrparteienhaus kaufen und hat bereits eine verbindliche Kaufzusage gemacht sowie die Finanzierungszusage etc. vorgelegt. Die Person möchte nun Einblick in die Protokolle der Eigentümergemeinschaft, um mehr über Renovierungen, Verwaltung etc. zu erfahren. Dies ist grundsätzlich zulässig. Entsprechend dem Grundsatz der Datenminimierung sind die Protokolle jedoch zu schwärzen, sodass keine personenbezogenen Daten sichtbar sind. Wenn diese Daten aber erforderlich sind oder eine Schwärzung extrem aufwändig wäre, ist es auf Grundlage der berechtigten Interessen möglich, die vollständigen Protokolle an den zukünftigen Eigentümer herauszugeben. Die Abwägung der Interessen dürfte zugunsten des Kaufinteressenten ausgehen, da jeder Eigentümer damit rechnen muss, dass Informationen zur Hausverwaltung an neue Eigentümer (auch kurz vor dem endgültigen Kauf) offengelegt werden müssen.

Datenverarbeitung durch eine humanitäre Stiftung

Eine liechtensteinische Stiftung verarbeitet unter anderem auch besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO zu humanitären und sozialen Zwecken. Konkret fördert die Stiftung fallweise Einzelpersonen mit der klassischen Einzelfallhilfe. In diesem Zusammenhang werden die personenbezogenen Daten, je nach den Umständen, entweder direkt bei der betroffenen Person oder über eine Drittperson bzw. eine Drittstelle erhoben und dann von der Stiftung geprüft, um zu bestimmen, ob die ersuchte finanzielle Unterstützung mit dem Stiftungszweck vereinbar ist. Die Stiftung stellte sich vor allem die Frage, auf welcher Rechtsgrundlage sie die indirekt erhobenen sensiblen Daten verarbeiten darf.

Aus Sicht der DSS bieten sich in Bezug auf Art. 9 Abs. 2 DSGVO mehrere Möglichkeiten an. Die Einwilligung gemäss Art. 9 Abs. 2 Bst. a DSGVO wäre der Idealfall, falls sich dies verwirklichen lässt. Eine weitere Option wäre die Verarbeitung zum Schutz lebenswichtiger Interessen gemäss Art. 9 Abs. 2 Bst. c DSGVO. Insbesondere ergänzt Erwägungsgrund 46, dass dieser Fall vor allem auf humanitäre Hilfe zutrifft. Der Erwägungsgrund besagt zwar des Weiteren, dass Art. 9 Abs. 2 Bst. c DSGVO nur zum Tragen kommt, wenn keine andere Rechtsgrundlage identifiziert werden kann. Aus dem geschilderten Sachverhalt lässt sich aber schliessen, dass die Einholung einer Einwilligung bisweilen auf Grund der Umstände nicht zu bewerkstelligen ist. Die dritte Alternative des Art. 9 Abs. 2 Bst. d DSGVO sah die DSS hingegen als kritisch an, da es sich bei den hier betroffenen Personen um Mitglieder der Organisation handeln muss oder zumindest um Personen, die in regelmässigem Kontakt mit der Stiftung stehen. Dies ist bei der Einzelfallhilfe gerade nicht erfüllt.

Zusammenfassend konnte daher festgestellt werden, dass für den beschriebenen Fall der Einzelfallhilfe die Grundlagen für die Datenverarbeitung in Art. 6 Abs. 1 Bst. b (vorvertragliche Massnahmen und Kontaktaufnahme bzw. Datenübermittlung durch die betroffene Person oder deren Vertreter) sowie Art. 9 Abs. 2 Bst. c DSGVO (humanitäre Hilfe und fehlende Möglichkeit der Einholung einer Einwilligung) zu finden sind.

Antrag auf Löschung personenbezogener Daten in einer Familienchronik

Eine Privatperson erkundigte sich bei der DSS, ob es zulässig sei, bei der zuständigen Gemeinde gemäss Art. 17 DSGVO zu beantragen, dass ihre personenbezogenen

Daten in der kommunalen Familienchronik gelöscht werden bzw. ob sie gegen die Verarbeitung ihrer Daten Widerspruch gemäss Art. 21 DSGVO einlegen könne.

Gemäss Art. 12 Abs. 2 Bst. f Gemeindegesetz fallen die Förderung des sozialen, kulturellen und religiösen Lebens, einschliesslich der Personen-, Familien- und genealogischen Forschung sowie der Führung und Veröffentlichung von Familienchroniken und Biografien, in den eigenen Wirkungsbereich der Gemeinden. Grundsätzlich kann die Gemeinde somit selbst oder über einen dafür zuständigen Verein etc. solche Familienbücher führen und veröffentlichen. Die Rechtsgrundlage dafür findet sich in Art. 6 Abs. 1 Bst. e DSGVO i.V.m. Art. 12 Abs. 2 Bst. f Gemeindegesetz.

Im Normalfall kann eine betroffene Person dagegen auf Grundlage von Art. 21 DSGVO Widerspruch einlegen, wenn sie dafür Gründe vorbringen kann, die sich aus ihrer besonderen Situation ergeben. Im vorliegenden Fall kommt allerdings die Ausnahme in Art. 21 Abs. 6 DSGVO zum Tragen. Diese betrifft konkret eine Datenverarbeitung zu einem historischen Forschungszweck, die zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist. Das Gemeindegesetz besagt in Art. 12, dass die Familienchronik zum eigenen Wirkungskreis der Gemeinde gehört und dieser umfasst alles, was das Interesse der Gemeinde berührt. Somit gibt es eine öffentliche Aufgabe und ein öffentliches Interesse. Es ist daher nicht möglich, Widerspruch dagegen einzulegen.

Betreffend das Recht auf Löschung in Art. 17 DSGVO ist es ebenso, dass dieses eingeschränkt ist. Hier besagt Abs. 1 Bst. c., dass Daten zu löschen sind, wenn eine betroffene Person gemäss Art. 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen. Nachdem der Widerspruch in dem Falle nicht möglich ist, kann auch das Recht auf Löschung gemäss Art. 17 Abs. 1 Bst. c DSGVO nicht geltend gemacht werden.

Trotz dieser rechtlichen Regelung empfiehlt die DSS den Gemeinden zu berücksichtigen, wenn jemand tatsächlich ganz spezielle Umstände vorbringt, warum er in der Chronik nicht aufscheinen will. In diesem Fall könnte etwa ein Platzhalter den Namen der betroffenen Person ersetzen.

Auskunftsrecht bei Unternehmen in Liquidation

Ein Treuhänder ist mit der Frage an die DSS herangetreten, ob das datenschutzrechtliche Auskunftsrecht nach Art. 15 DSGVO bei einem liquidierten Unternehmen weiter besteht und wer dieses zu gewähren sowie allfällige damit verbundene Kosten zu tragen hat. Grundsätzlich besteht das Auskunftsrecht eines Betroffenen auch während bzw. nach der Liquidation eines Unternehmens weiter, so lange die personenbezogenen Daten noch irgendwo lagern bzw. gespeichert sind. Auskunft erteilen muss der Verantwortliche bzw. derjenige, der in dessen Namen handelt. Dies kann auch ein eingesetzter Liquidator sein. Weiter ist die datenschutzrechtliche Auskunft dem Betroffenen kostenlos zu erteilen (Art. 12 Abs. 5 DSGVO). Nur in Ausnahmefällen (offenkundige Unbegründetheit oder Exzessivität der Auskunftsgesuche) kann ein angemessenes Entgelt verlangt werden.

Ein Verantwortlicher kann sich jedoch allenfalls auf die Ausnahme in Art. 34 Abs. 1 Bst. b Ziff. 1 und Abs. 2 DSG berufen und die Auskunft verweigern. Diese gilt bei personenbezogenen Daten, die nur noch deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmässiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen und bei denen die Auskunftserteilung einen unverhältnismässigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Massnahmen ausgeschlossen ist. Die Gründe der Auskunftsverweigerung sind jedoch zu dokumentieren und der betroffenen Person mitzuteilen. Die Bedingung des unverhältnismässigen Aufwands wird allerdings von den Gerichten sehr streng ausgelegt, das heisst, es muss schon ein wirklich unzumutbarer Aufwand vorliegen, damit er als unverhältnismässig anerkannt wird und in einem Beschwerdeverfahren bzw. vor Gerichten Bestand hätte.

Öffnung von Postsendungen an abwesende Mitarbeitende

In einer Organisation war ein Mitarbeitender krankheitsbedingt länger ausgefallen und es stellte sich die Frage, wie mit an diesen adressierter Post umzugehen sei. Darf sie geöffnet werden, um eventuell beiliegende Rechnungen bezahlen zu können? Zunächst muss dazu geklärt werden, ob es sich um geschäftliche Postsendungen handelt oder private (die ins Büro geliefert wurden). Geschäftliche Sendungen «gehören» nämlich dem Arbeitgeber, und aus diesem Grund ist dieser auch berechtigt, solche Sendungen zu öffnen. Dazu wird keine Einwilligung des betroffenen Mitarbeitenden benötigt. Bei privaten Postsendungen dagegen braucht es eine solche Einwilligung.

Ist es den Mitarbeitenden einer Organisation also erlaubt, sich auch private Post ins Büro schicken zu lassen, so dürfen solche Sendungen nicht ohne die Einwilligung des betroffenen Mitarbeitenden geöffnet werden. Dies gilt auch dann, wenn unklar ist, ob es sich um eine geschäftliche oder private Sendung handelt. Kann mit dem abwesenden Mitarbeitenden nicht

geklärt werden, ob sämtliche (auch ev. private) an ihn gerichteten Postsendungen geöffnet werden dürfen (oder welche Postsendungen / Absender allenfalls auch nicht), so darf zumindest alles, was eindeutig geschäftliche Belange betrifft, geöffnet werden.

Herausgabe OP-Bericht durch Spital

Ein Spital wurde vermehrt über das Kontaktformular seiner Webseite angefragt, Austrittsberichte oder Operationsberichte von ehemaligen Patienten an diese zu übermitteln. Obwohl das Spital solche Berichte aus Sicherheitsgründen nur via Post an die beim Spital hinterlegte Postadresse des betroffenen Patienten / (vermeintlichen) Auskunftsersuchenden schickt, stellt sich die Frage, ob im Falle von Anfragen über das Kontaktformular der Webseite zusätzlich noch eine Identifikation der auskunftssuchenden Person via ID-Kopie durchgeführt werden müsste. Anders als bei telefonischen Anfragen oder bei persönlicher Vorsprache, wo unmittelbar mit gezielten Rückfragen eine Identifikation vorgenommen werden kann, ist dies bei Anfragen via Kontaktformular nicht möglich.

Aus Sicht des Datenschutzes ist festzustellen, dass es sich bei den angefragten Berichten zwar einerseits um sehr sensible Gesundheitsdaten handelt, die keinesfalls an unberechtigte Personen gelangen dürfen und die eine zusätzliche Identifikation mit ID-Kopie durchaus rechtfertigen würden. Andererseits hat das Spital aber durch den Wechsel des Kommunikationskanals sichergestellt, dass die Berichte nur an die betroffene Person geschickt werden, unabhängig davon, wer sie via Kontaktformular angefragt hat. Eine unberechtigte Person müsste dann schon die Post abfangen oder in den Briefkasten einbrechen, um an den Bericht zu gelangen. Das Vorgehen des Spitals, Anfragen aus dem Kontaktformular nicht via E-Mail, sondern via Post zu beantworten, erscheint daher datenschutzrechtlich ausreichend abgesichert. Würden die Dossiers jedoch vom Spital via E-Mail verschickt, wäre in jedem Fall vorher eine Identifikation mittels ID-Kopie vorzunehmen, sowie natürlich auch eine entsprechende Verschlüsselung des E-Mails.

Sammeln von Briefmarken (und Postkarten)

Eine Privatperson wandte sich mit der Frage an die DSS, was beim Sammeln von Briefmarken und Postkarten datenschutzrechtlich zu beachten sei, insbesondere wenn ihr die Briefe und Postkarten von Unternehmen, beispielsweise aus einem vergangenen Preisausschreiben, überlassen werden. Das Sammeln von Briefmarken erscheint datenschutzrechtlich unproblematisch, weil die Marken in den allermeisten Fällen von den Briefkuverts und Postkarten abgelöst werden (und diese dabei vernichtet werden) und somit keine personenbezogenen Daten verarbeitet werden. Auch wenn in Einzelfällen ein Briefcouvert oder eine Postkarte mit einer speziellen Marke im Original mit aufbewahrt werden sollte, wäre dies wohl datenschutzrechtlich noch zu rechtfertigen, sofern keine systematische Ordnung nach den darauf ersichtlichen Adressdaten erfolgt.

Anders sieht es jedoch aus, wenn Postkarten mit Absenderadressen gesammelt werden, in vielfacher gleicher Ausführung und mehrheitlich dem gleichen (aufgedruckten) Wertzeichen darauf. Ein wichtiges Unterscheidungsmerkmal dieser Karten sind dann nebst dem Stempel und der Frankatur auch die Namen und Adressen der Absender. Und somit sind die personenbezogenen Daten der Absender auch ein zentrales Kriterium, nach dem die Karten in einer Sammlung sortiert werden könnten, selbst wenn es dabei nicht um die Kenntnis der betroffenen Personen geht. Dies wiederum entspricht aber einer systematisierten Verarbeitung dieser Daten und untersteht deshalb dem Datenschutzrecht (Art. 2 Abs. 1 DSGVO). Es braucht daher für die Verarbeitung eine Rechtsgrundlage, was in diesem Fall nur die Einwilligung der Absender sein kann. Wenn diese nicht vorliegt und auch nicht mehr eingeholt werden kann, darf ein Unternehmen dem Sammler Postkarten nur mit geschwärzten Absenderadressen überlassen. Datenschutzrechtlich nicht relevant sind dagegen personenbezogene Daten bereits verstorbener Menschen.

2.5 Auswahl konkreter technischer Fragen

Von den zahlreichen Fragen zu technischen Themen wurden die folgenden drei im Berichtsjahr häufig gestellt:

Angemessene Berücksichtigung des «Stands der Technik» bei der Umsetzung von technischen und organisatorischen Massnahmen

Da es weder in der DSGVO noch im DSG eine konkrete Definition des Begriffs «Stand der Technik» gibt, wandten sich auch im Jahr 2022 einige Unternehmen an die DSS, um Informationen darüber zu erhalten, wie diese Anforderung in der Praxis umgesetzt werden kann.

Die Feststellung, ob technische und organisatorische Massnahmen (TOMs) angemessen und geeignet sind, kann für Verantwortliche und Auftragsverarbeiter schwierig sein, da es keine gesetzlichen Schwellenwerte oder standardisierten Messmethoden zur Bewertung dieser gibt. Die DSGVO legt bei der Auslegung des Begriffs «Stand der Technik» besonderen Fokus auf eine sorgfältige Überprüfung und Beurteilung der TOMs, die im jeweiligen Einzelfall erforderlich, geeig-

net und angemessen sind, um personenbezogene Daten zu schützen. Es geht dabei nicht ausschliesslich darum, die dominierende Meinung unter technischen Experten zu ermitteln, sondern auch um die Einschätzung von technischen Debatten und um die Evaluation von am Markt verfügbaren, technischen Alternativen. Es ist nicht erforderlich, dass die neuesten Erkenntnisse aus Wissenschaft und Forschung umgesetzt werden, da die Erfüllung des «Stand der Technik» auch an eine gewisse Anerkennung und Bewährung der in der Praxis vorhandenen Massnahmen gekoppelt ist. Im Kontext der DSGVO ist es überdies zulässig, bei der Wahl der TOMs – neben weiteren Faktoren – auch wirtschaftliche Aspekte zu berücksichtigen. Die Wirtschaftlichkeit einer Massnahme kann jedoch nur durch die individuelle Überprüfung des Schutzbedarfs und der Realisierungskosten ermittelt werden. Diese Abwägung muss rechtlich durchgeführt und dokumentiert werden und erfordert daher in der Regel die enge Zusammenarbeit zwischen Technikern und Juristen.

Weitere nützliche Informationen zu diesem Thema, insbesondere zur Erklärung des Begriffs «Stand der Technik» im Kontext der DSGVO sowie zur Bereitstellung von praxisorientierten Hilfestellungen und empfohlenen weiterführenden Literaturquellen, stellt die DSS auf ihrer Internetseite zur Verfügung.

DSGVO-Konformität bestimmter Einwilligungsplattformen bzw. CMP-Plattformen (Cookie-Banner)

Die DSS erhielt im Jahr 2022 mehrfach Anfragen bezüglich der DSGVO-Konformität von Einwilligungsplattformen bzw. CMP-Plattformen sowie zur Geeignetheit dieser Plattformen, um rechtskonforme Einwilligungen zur Datenverarbeitung einzuholen.

Bei Untersuchungen im Zusammenhang mit derartigen Anfragen hat die DSS wiederholt festgestellt, dass zahlreiche spezialisierte Anbieter von CMP-Plattformen bereits bei der Bereitstellung ihrer Dienste gegen Vorgaben der DSGVO verstossen. So wurde beispielsweise mehrfach festgestellt, dass einige Anbieter ihre Server zur Bereitstellung ihrer Dienste in unsicheren Drittländern wie den USA betreiben oder weitere Unterauftragsverarbeiter in unsicheren Drittländern in ihre Plattformen integrieren.

Die Verwendung von CMP-Plattformen kann für Webseitenbetreiber zudem weitere datenschutzrechtliche Problematiken aufwerfen, wenn die Standardkonfigurationen der CMP-Software nicht den Anforderungen der DSGVO entsprechen. Die österreichische Datenschutzorganisation «noyb» hat in diesem Zusammenhang bei 18 Datenschutzbehörden Beschwerden gegen 226 Webseiten eingereicht, welche die weit verbreitete CMP-Software «OneTrust» für den Cookie-Banner verwenden. noyb kritisierte dabei sowohl «irreführende Einstellungen» als auch unlautere Designtricks (sogenannte «Deceptive Design Patterns»), die in der CMP-Software von «OneTrust» nach Einschätzung der österreichischen Datenschutzorganisation zur Anwendung gelangten. Irreführende Cookie-Banner versuchen in der Regel, die Zustimmung der Webseitenbesucher zu erzwingen, indem unter anderem das Ablehnen von Cookies möglichst erschwert wird.

Datenschutzkonforme Nutzung von Google Analytics mit sogenannten Proxy-Lösungen

Auch im Berichtsjahr war eine der häufigsten Fragen, ob Google Analytics DSGVO-konform eingesetzt werden kann. Die DSS hat deshalb im März 2022 auf ihrer Internetseite eine Newsmeldung sowie einen Gastbeitrag im Volksblatt zu diesem Thema veröffentlicht.

Verschiedene Unternehmen sind im Verlauf des Berichtsjahres mit alternativen Lösungsansätzen im Zusammenhang mit Google Analytics auf die DSS zugekommen und haben um eine datenschutzrechtliche Einschätzung der DSS gebeten. Zusammengefasst handelte es sich in der Regel um Proxy-Lösungen. Die grundlegende Idee ist, dass eine dazwischengeschaltete Instanz (Proxy-Server) die an Google (Analytics) zu übermittelnden personenbezogenen Daten vorgängig anonymisiert bzw. löscht. Somit sollte Google keinen Personenbezug zu den Webseitenbesuchern mehr herstellen können – so die Idealvorstellung.

Bei genauer Betrachtung der diversen Lösungen gibt es jedoch einige Stolpersteine, vor allem technischer Natur, die es zu beachten gilt. In diesem Zusammenhang hat die Französische Aufsichtsbehörde (CNIL) einen interessanten Beitrag auf ihrer Internetseite veröffentlicht: https://www.cnil.fr/en/google-analytics-and-data-transfers-how-make-your-analytics-tool-compliant-gdpr. In diesem Beitrag wird einerseits näher auf die rechtliche Ausgangslage sowie die technischen Anforderungen von Proxy-Lösungen eingegangen, andererseits wird auf das vom EDSA veröffentlichte Dokument «Empfehlungen 01/2020 zu Massnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten» weiterverwiesen. Neben den technischen Hürden stellt sich aus Sicht der Verantwortlichen (Webseitenbetreiber) letztlich die Frage, ob mit dem Einsatz einer Proxy-Lösung noch ein Mehrwert geschaffen werden kann bzw. ob sich der finanzielle Aufwand hinsichtlich der Umsetzung lohnt.

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

3. Stellungnahmen zu Vorlagen und Erlassen

Die DSS begutachtete im Berichtsjahr insgesamt 25 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.

«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 die an sie gestellten Anforderungen im Berichtsjahr mit dem bestehenden Personal von 700 Stellenprozenten gut erfüllen. Die bereits in den Vorjahren praktizierte intensive Zusammenarbeit zwischen Technik und Recht war auch im Berichtsjahr unabdingbar für die meisten Tätigkeiten. Insbesondere die Frage nach der Zulässigkeit von Webanalyse-Tools etc. war beispielsweise fast täglich präsent und die Beurteilung von Datentransfers in ein unsicheres Drittland 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 zwei Fällen wieder je einen Experten zwecks Evaluierung eines anderen Schengen-Staates.

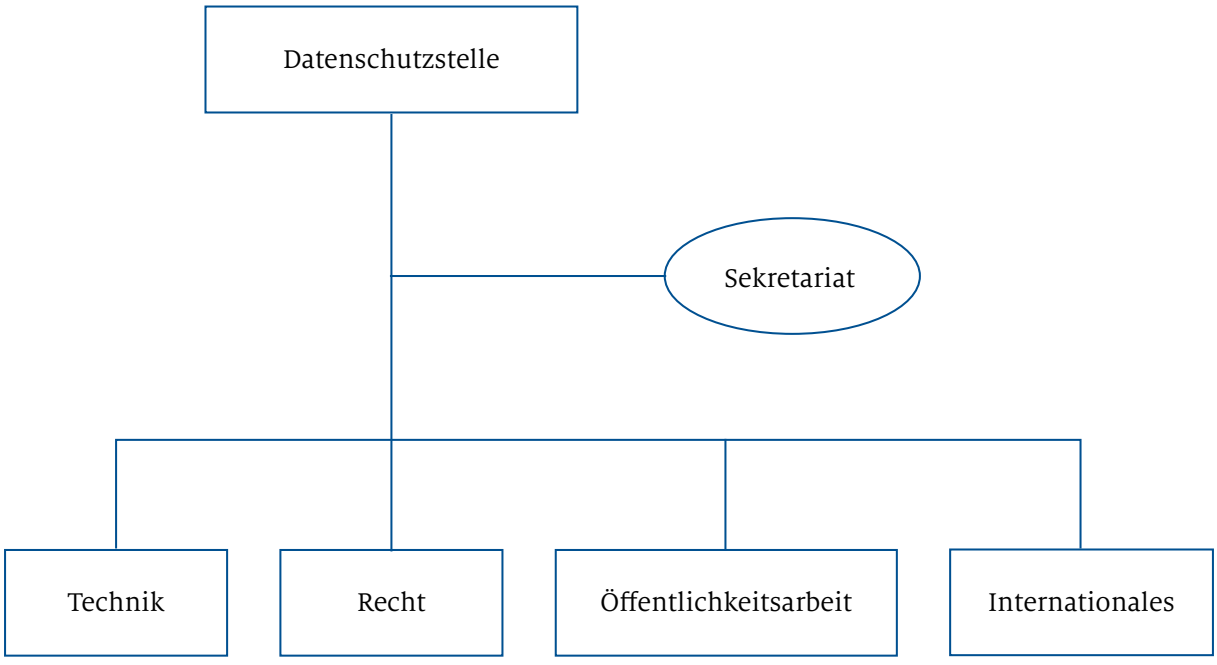


Abbildung 3: Organigramm Datenschutzstelle

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

5. Aufsicht, Beschwerden und Meldungen von Datenschutzverletzungen

5.1 Aufsicht

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

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

5.1.1 Amtswegige Überprüfungen bei Unternehmen

Aufgrund der schwierigen Lage vieler Unternehmen während der Covid-19-Pandemie hatte die DSS 2021 noch entschieden, von amtswegigen Überprüfungen bei Unternehmen abzusehen, ausser in jenen Fällen, in denen die DSS Informationen von Privatpersonen oder anderen Behörden in Bezug auf einen vermeintlichen Datenschutzverstoss erhielt, die Informanten aber keine formelle Beschwerde im Sinne des Art. 77 DSGVO einbringen wollten. Im Berichtsjahr nahm die DSS diese Praxis aber wieder auf und führte bereits zum zweiten Mal eine Serie amtswegiger Überprüfungen bei Unternehmen durch. Dafür wurden Anfang Herbst zwanzig mittelständische Unternehmen nach dem Zufallsprinzip ausgewählt. Diese Unternehmen erhielten einen standardisierten Fragebogen, mit dem überprüft wurde, inwieweit die Verantwortlichen die gesetzlichen Vorgaben der DSGVO in verschiedensten Bereichen erfüllt haben (z.B. Rechtsgrundlagen der Verarbeitung personenbezogener Daten, Führung des Verzeichnisses der Verarbeitungstätigkeiten, Informationspflichten gegenüber Betroffenen, Umsetzung der Betroffenenrechte, Datensicherheit, Auftragsverarbeitungsverträge, technische und organisatorische Massnahmen etc.). Da die Verantwortlichen zu diesem Zeitpunkt bereits mehrere Jahre Zeit gehabt hatten, diese verpflichtenden Vorgaben umzusetzen, war von der DSS erwartet worden, dass dieser sehr allgemein gehaltene Prüfungsdurchgang für die Unternehmen keine allzu grosse Hürde darstellen sollte. Zudem hatte die DSS bereits zuvor auf den für die amtswegigen Überprüfungen verwendeten Fragebogen mittels Newsletter hingewiesen und ihn auf ihrer Internetseite für eine Selbstevaluation zur Verfügung gestellt. Die ersten Ergebnisse der Überprüfung waren jedoch ernüchternd. Kein einziges der geprüften Unternehmen wies eine vollkommen einwandfreie Umsetzung der datenschutzrechtlichen Pflichten auf, doch liess sich bei rund einem Viertel der geprüften Unternehmen immerhin feststellen, dass zumindest in den zentralen Punkten eine annehmbare Umsetzung erfolgt war. Die übrigen Unternehmen konnten jedoch nur eine schlechte oder gar keine Umsetzung zentraler datenschutzrechtlicher Pflichten vorweisen. Die DSS plant daher für das Folgejahr die Öffentlichkeitsarbeit erneut zu verstärken, um die Unternehmen mit grossem Nachdruck darauf hinzuweisen, dass nach knapp fünf Jahren Geltung der DSGVO und des DSG eine fehlende Umsetzung der darin enthaltenen Pflichten nicht mehr entschuldbar ist.

5.1.2 Amtswegige Kontrolle von Fahndungen der Landespolizei (Art. 36 SIS II-Beschluss)

Im Rahmen ihrer amtswegigen Kontrolltätigkeit führte die DSS im November eine Kontrolle in Bezug auf Art. 36-Fahndungen des SIS II-Beschlusses[1] bei der Landespolizei des Fürstentums Liechtenstein durch. Als Grundlage diente der Entscheid der «SIS II Supervision Coordination Group» (SCG) aus dem Jahr 2019, eine koordinierte Kontrolle in Bezug auf Art. 36-Fahndungen durchzuführen. Zu diesem Zweck wurde ein Fragebogen erstellt, welcher als Anleitung und Hilfestellung für die Datenschutz-Aufsichtsbehörden dienen sollte. Grundsätzlich handelt es sich jedoch um eine Vor-Ort-Kontrolle, an der einzelne Fälle überprüft werden sollen. Die Kontrolle sollte ursprünglich die

1 Beschluss (EU) Nr. 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II).

Jahre 2015 – 2019 abdecken. Aufgrund der Covid-19-Pandemie wurde die Frist zur Durchführung der Kontrolle jedoch mehrfach verlängert. Die DSS hat sich daher entschieden, die Kontrolle auf die Jahre 2015 – 2021 auszudehnen.

Die zu überprüfende Stelle ist die jeweilige nationale Behörde, welche für die Erstellung der Art. 36-Fahndungen verantwortlich ist. In Liechtenstein ist dies die Landespolizei im Rahmen der Internationalen Polizei Kooperation (IPK). Aufgrund der Antworten auf den Fragebogen hat die DSS entschieden, neun Fälle während der Vor-Ort-Kontrolle näher zu prüfen. Im Rahmen dieser Kontrolle wurde lediglich ein Mangel festgestellt, der jedoch von der IPK schon vorgängig und eigenständig erkannt und behoben worden war. Art. 17 Abs. 2 DSG erlaubt der DSS von Beanstandungen abzusehen, wenn es sich um inzwischen beseitigte Mängel handelt. In diesem Sinne sah die DSS keine Notwendigkeit, Empfehlungen oder Massnahmen auszusprechen.

5.1.3 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. Seit Juni 2019 wurde die entsprechende Fachstelle der Landespolizei aufgebaut und ist seit Januar 2020 voll funktionsfähig. Aufgrund der Sensibilität der zu verarbeitenden personenbezogenen Daten und der daraus resultierenden Folgen, sprich dem sich aus einer Datenverarbeitung ergebenden Risiko für die betroffene Person, hat die DSS im Berichtsjahr entschieden, nach einer zweijährigen Anfangsphase das Bedrohungsmanagement einer Datenschutzüberprüfung zu unterziehen. Diese umfasste datenschutzrechtliche wie auch technische Aspekte. Nach einem Vorgespräch mit den Verantwortlichen der Landespolizei hat die DSS Ende des Berichtsjahres die Datenschutzüberprüfung eröffnet. Mit Frist bis Ende Februar 2023 ersuchte die DSS um Einreichung der relevanten Dokumente, Statistiken und Regelwerke wie auch um die Beantwortung eines Fragebogens. Diese Informationen sind die Grundlage für eine erste Dokumentenprüfung durch die DSS. Gestützt hierauf soll anschliessend eine Vor-Ort-Kontrolle durchgeführt werden. Die DSS wird im nächsten Tätigkeitsbericht über das Ergebnis informieren.

5.1.4 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 anderen Fällen von Datenverarbeitungen. Die Grenze ist oft fliessend, da die betroffenen Personen selbst nicht immer sicher sind, ob sie wirklich eine formelle Beschwerde einbringen wollen. Die DSS akzeptiert daher auch bereits «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 datenschutzkonform umgesetzt werden. Unter anderem ging es um eine Kamera, die einen Schrebergarten miterfasste, Kameras an Wohnhäusern wie auch eine Baustellenüberwachung. Bei letzterer war nirgends signalisiert und somit erkennbar, wer diese Kamera betreibt. Der Fall verdeutlichte daher erneut die Wichtigkeit einer transparenten Information bezüglich der Datenverarbeitungen (Art. 13 DSGVO).

5.1.5 Schengen-Evaluationen in Spanien und Schweden

Für die regelmässige datenschutzrechtliche Evaluation der diversen europäischen Informationssysteme in den Mitgliedstaaten wird jeweils ein Expertenteam bestehend aus Mitarbeitenden der EU-Kommission wie auch der EU/EWR-Aufsichtsbehörden zusammengestellt, welches eine Vor-Ort-Kontrolle durchführt. Im Rahmen dieser Schengen-Evaluationen (Schengen-Acquis) entsandte die DSS im März einen Juristen nach Spanien sowie im Juni einen IT-Experten nach Schweden, um dort die Einhaltung geltender Datenschutzbestimmungen durch die Informationssysteme zu überprüfen. Unter der Leitung der Generaldirektion Migration und Inneres (DG Home) der EU-Kommission führte in beiden Fällen eine Expertengruppe während einer Woche vor Ort Begehungen sowie Interviews mit den Behörden und deren IT-Dienstleistern durch. Gegenstand der Untersuchungen waren Datenverarbeitungsvorgänge im Zusammenhang mit dem Schengener Informationssystem der zweiten Generation (SIS II) sowie des Visa Informationssystems (VIS). Vor der eigentlichen Vor-Ort-Inspektion beantworteten die überprüften Behörden unter anderem bereits einen umfangreichen Fragebo-

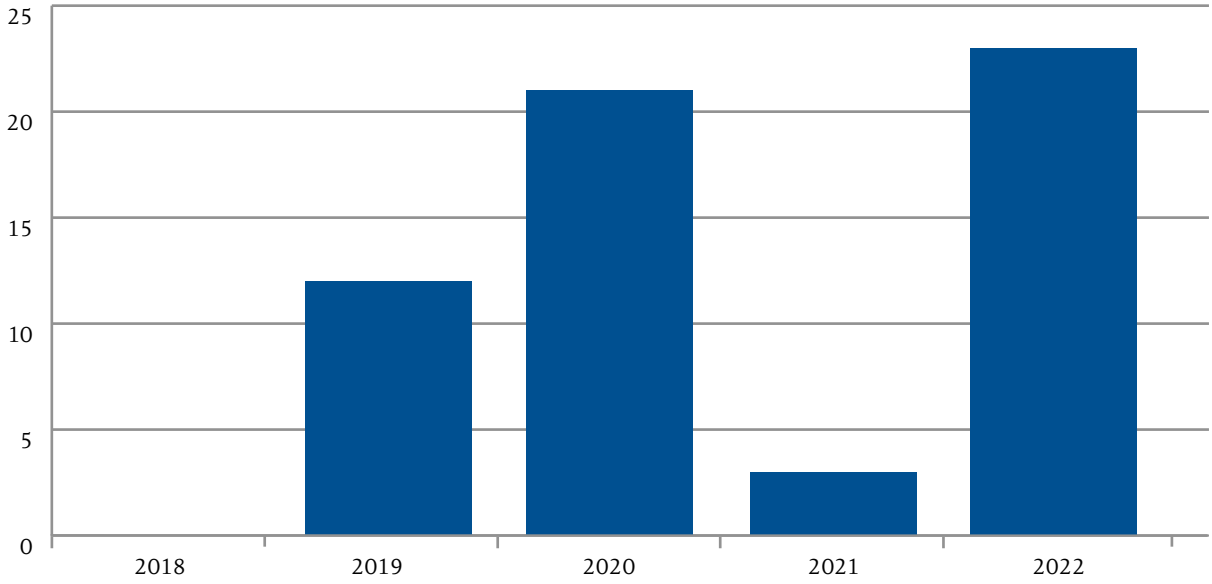


Abbildung 4: Anzahl der Datenschutzüberprüfungen pro Jahr

gen, so dass sich die Experten vorab ein gutes Verständnis der Ausgangslage verschaffen konnten. Das Wochenprogramm wurde von den Datenschutzbehörden vor Ort zusammengestellt. Ebenso begleiteten Delegierte der Datenschutzbehörden die Expertengruppen während der ganzen Woche. Jede Expertengruppe verfasste im Rahmen ihrer Arbeit bereits vor Ort den Entwurf des Evaluierungsberichts. Gemäss den Verfahrensschritten des Schengen-Evaluierungsmechanismus haben die überprüften Behörden nach Zustellung des Entwurfs zwei Wochen Zeit, eine Stellungnahme dazu abzugeben.

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 37 Beschwerden von Privatpersonen, die sich direkt an die DSS als zuständige Aufsichtsbehörde für ein liechtensteinisches Unternehmen oder eine öffentliche Stelle richteten. Die Beschwerdeführer hatten zum überwiegenden Teil ihren Wohnsitz in Liechtenstein. Aber auch Personen aus dem EU/EWR-Raum, vor allem Deutschland und Österreich, brachten Beschwerden bei der DSS ein. Zusätzlich erhielt die DSS im Rahmen der Zusammenarbeit mit den anderen Aufsichtsbehörden im EU/EWR-Raum unter Art. 56 ff. DSGVO im Berichtsjahr drei weitere Beschwerden von Personen aus einem anderen Mitgliedstaat, die sich jeweils gegen ein liechtensteinisches Unternehmen richteten.

Nicht eingerechnet in diese Zahl sind Anfragen von betroffenen Personen, bei denen sich herausstellte, dass die Beschwerde keine Verarbeitung von sie persönlich betreffenden personenbezogenen Daten zur Grundlage hatte. Damit lag die Anzahl der Beschwerden gemäss Art. 77 DSGVO bei der DSS rund 30% unter der Anzahl des Vorjahres.

Auch 2022 konzentrierten sich die Beschwerdeverfahren 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. Geldbussen wurden 2022 keine verhängt. Damit ist die DSS 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 abschreckend» 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:

Ein Beschwerdeführer machte geltend, dass die DSS erkennen möge, dass entgegen der Ausführungen in einer Datenschutzerklärung eine andere Stelle als Verantwortlicher gemäss Art. 4 Ziff. 7 DSGVO zu gelten habe.

Art. 4 Ziff. 7 DSGVO definiert den «Verantwortlichen» als «die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet». Diese Stelle ist dann unter anderem in der Information an die betroffenen Personen gemäss Art. 13 Abs. 1 Bst. a DSGVO anzugeben. Im konkreten Fall fand sich auf der betreffenden Internetseite die Datenschutzerklärung mit der Information, dass die Beschwerdegegnerin die verantwortliche Stelle im Zusammenhang mit der Datenverarbeitung sei. Selbst wenn es im Impressum heisst, dass es in Bezug auf die gegenständliche Seite einen Auftrag einer weiteren Stelle gibt, ist diese Information bzw. der allgemein verwendete Begriff «Auftrag» im Impressum nicht mit der datenschutzrechtlichen Verantwortlichkeit bzw. einer Auftragsverarbeitung gemäss Art. 28 DSGVO gleichzusetzen. Grundsätzlich sind die in Art. 4 Ziff. 7 DSGVO genannten natürlichen oder juristischen Personen, Behörden, Einrichtungen oder andere Stellen frei, selbst zu entscheiden, ob sie die

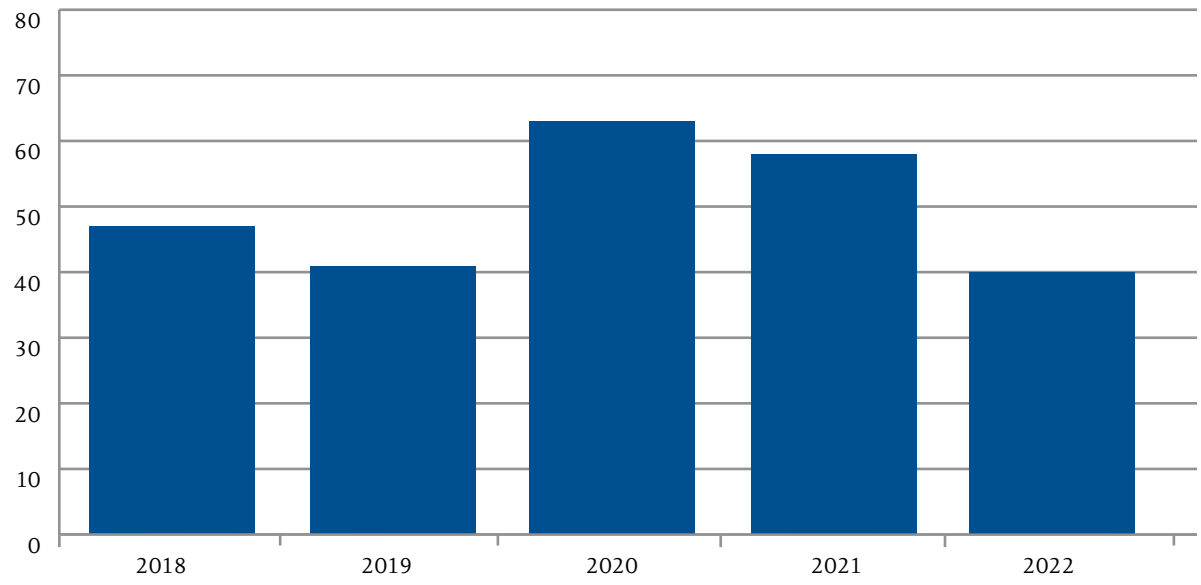


Abbildung 5: Anzahl der Beschwerden pro Jahr

Verantwortlichkeit für eine bestimmte Datenverarbeitung tragen wollen. Entscheidend aus Sicht des Datenschutzes ist, dass es für *jede* Datenverarbeitung *einen bestimmten* Verantwortlichen geben muss, dem dann auch die Rechenschaftspflicht obliegt. Es kann somit nicht sein, dass ein Beschwerdeführer bestimmt, wer als verantwortliche Stelle zu gelten hat. Wenn eine Stelle diese Rolle eindeutig (insbesondere mittels Information gemäss Art. 13 DSGVO) übernommen hat und damit auch die Rechenschaftspflicht im Sinne des Art. 5 Abs. 2 DSGVO wahrnimmt, kann diese Entscheidung nicht in Frage gestellt werden. Vor allem auch dann nicht, wenn es für den Beschwerdeführer keinerlei Nachteil mit sich bringt, wenn eine bestimmte Stelle die Verantwortung übernimmt. Es besteht somit kein subjektives Recht einer betroffenen Person bzw. des Beschwerdeführers, dass die Aufsichtsbehörde mittels Behördenentscheidung bestimmte Stellen oder Personen als Verantwortliche im Sinne des Art. 4 Ziff. 7 DSGVO bestimmt.

In mehreren Beschwerden ging es um die Frage der Zulässigkeit einer Nicht-Verschlüsselung einer Webseite und die unsichere http-Verbindung.
Zum Zeitpunkt der Beschwerdeeinbringung wurde beim Betrieb der betreffenden Internetseite nicht durchgängig eine datenschutzkonforme Verschlüsselung (https mittels SSL/TLS) eingesetzt. Somit bestand für Besucher und Besucherinnen der Internetseite das Risiko, mittels Kontaktformular personenbezogene Daten einzugeben und diese anschliessend über das unsichere Medium Internet zu versenden. Dadurch war die Vertraulichkeit der zu übermittelnden Daten nicht sichergestellt. Art. 25 DSGVO verlangt jedoch, dass der Verantwortliche – unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen – sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Massnahmen trifft, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen. Den Anforderungen der DSGVO wird in dieser Hinsicht entsprechend dem Stand der Technik üblicherweise mittels des «HyperText Transfer Protocol Secure», kurz «HTTPS», Rechnung getragen. Es handelt sich dabei um ein sicheres Hypertext-Übertragungsprotokoll, mit dem Daten sicher übertragen werden können. HTTPS dient dem Herstellen von Vertraulichkeit und Integrität zwischen einem Web-Server (dem Server, der die Webseite bereitstellt) und einem Client (z.B. dem Web-Browser eines Benutzers). Die Vertraulichkeit und Integrität werden unter anderem durch Verschlüsselung und Authentifizierung erreicht. Die von der Beschwerdegegnerin zum Zeitpunkt der Beschwerdeeinbringung eingesetzten Übertragungsmechanismen entsprachen somit nicht dem von Art. 25 DSGVO geforderten Standard.

Ein Beschwerdeführer brachte vor, dass die «Rechtmässigkeit» des Covid-19-Zertifikates in seiner aktuellen technischen Umsetzung verletzt sei, da die mittels QR-Code gespeicherten Gesundheitsdaten durch unqualifizierte Dritte ausserhalb des Gesundheitsbereiches eingesehen, verarbeitet und gespeichert werden könnten.

Die Prüfung durch die DSS ergab, dass in der Praxis für die betroffenen Personen tatsächlich das Risiko besteht, dass ein Prüfer des Covid-19-Zertifikates – entgegen den Vorgaben der Covid-19-Verordnung und unter Zuhilfenahme von nicht zugelassenen Methoden – unbefugt auch die weiteren im QR-Code enthaltenen Informationen (wie Gesundheitsdaten) ausliest und möglicherweise auch abspeichert. Um dies zu bewerkstelligen, kann sich ein Prüfer an Stelle der zugelassenen «Prüf-App» etwa einer App zur Speicherung von Covid-19-Zertifikaten oder einer speziellen Software zur Dekodierung der QR-Codes auf den Covid-19-Zertifikaten bedienen. Daraus folgte, dass die «Quelle» des Risikos für die betroffene Person darin besteht, dass durch unbefugtes Auslesen des Covid-19-Zertifikats durch einen Prüfer Gesundheitsdaten erhoben werden können, und zwar bezüglich der Covid-19-Impfung und/oder eines Covid-19-Testergebnisses bzw. der Genesung. Neben dem Vorhandensein einer Impfung, eines Testergebnisses oder einer Genesung kann auch der Zeitpunkt davon erhoben werden. Um festzustellen wie hoch das Risiko ist, war in weiterer Folge zu prüfen, welche Schäden für die betroffene Person aus dieser Möglichkeit der unbefugten Einsichtnahme entstehen können. Nach Berücksichtigung aller Umstände stellte die DSS fest, dass ein möglicher Schaden in einem Kontrollverlust bzw. dem Verlust der Vertraulichkeit der entsprechenden Gesundheitsdaten bestehen kann. In Bezug auf den Kontrollverlust konnte aber festgestellt werden, dass eine betroffene Person doch eine Kontrolle über den Prüfvorgang hat. Sie kann diesen aufmerksam beobachten und auch durch Nachfrage beim Prüfer sicherstellen, dass dieser eine zugelassene Prüf-App verwendet. Auf Grund des geringen Umfangs der unbefugt zu erlangenden Daten ist zudem mit grosser Wahrscheinlichkeit auszuschliessen, dass es zu gewichtigeren Schäden wie etwa Rufschädigung, Diskriminierung, Profilbildung etc. kommt. Ein erheb-

licher gesellschaftlicher Nachteil ist ebenfalls unwahrscheinlich, da die unbefugte Offenlegung einer Impfung, Testung oder Genesung nach allgemeiner Lebenserfahrung nicht mit Diskriminierung, Ausgrenzung oder Abwertung verbunden ist. Dem Risiko sowie dem möglichen Schaden gegenüberzustellen ist jedoch der Zweck des Zertifikats, nämlich den grenzüberschreitenden Personenverkehr sowie die Aufrechterhaltung des kulturellen und gesellschaftlichen Zusammenlebens während der COVID-19-Pandemie zu erleichtern und zugleich ein hohes Niveau des Schutzes der öffentlichen Gesundheit zu gewährleisten.

Zusammenfassend stellte die DSS fest, dass im gegebenen Fall zwar ein geringes Risiko sowie eine geringe Eintrittswahrscheinlichkeit eines unbefugten Zugriffs auf die Gesundheitsdaten im QR-Code des Covid-19-Zertifikats gegeben ist. Unter Abwägung aller weiteren Faktoren wie dem Stand der Technik, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung war aber festzustellen, dass die getroffenen technischen und organisatorischen Massnahmen eine geeignete Massnahme darstellten, um die Datensicherheit in angemessenem Umfang zu schützen.

Ein Beschwerdeführer machte geltend, dass an den Schulen in Liechtenstein unter Verletzung der Datenschutzbestimmungen Lernapplikationen zum Einsatz kämen, welche entweder von amerikanischen Anbietern stammen oder welche Tracking-Tools einsetzen.

Im vorliegenden Fall hatte die Beschwerdegegnerin die Nutzung bestimmter US-amerikanischer Lernapplikationen im Schulunterricht auf Grundlage des Art. 6 Abs. 1 Bst. e DSGVO zur Erfüllung ihrer gesetzlichen Aufgaben angeordnet und zusätzlich weitere Lernapplikationen ausgewählt, die Trackingtools einsetzen, mittels derer personenbezogene Daten der Schüler und Schülerinnen an Drittfirmen wie Google mit Sitz in den USA übermittelt werden. Die Beschwerdegegnerin nimmt den Datentransfer zwar nicht direkt selbst vor und setzt auch selbst keine Tracking-Tools ein, sie entscheidet aber auf Grund der Wahl der eingesetzten Mittel, dass es zu einem solchen Transfer kommt. Das Verhältnis zwischen der Beschwerdegegnerin und den Anbietern der Applikationen lässt sich als Auftragsverarbeitung im Sinne des Art. 28 DSGVO qualifizieren. Soweit diese Auftragsverarbeiter Trackingtools einsetzen, sind die Anbieter von letzteren in Bezug auf die Beschwerdegegnerin als Unterauftragsverarbeiter zu qualifizieren. Seitens Beschwerdegegnerin konnte nicht überzeugend dargelegt werden, dass sie vertragliche, organisatorische und technische Massnahmen implementiert hat, um diesen Datentransfer im Rahmen des Tracking auszuschliessen. Es wird vielmehr der Eindruck erweckt, dass die Beschwerdegegnerin wenig bis gar keinen Einfluss hat, wie und in welchem Ausmass sowie unter Einsatz welcher zusätzlichen Massnahmen die genannten Applikationen und Portale personenbezogene Daten in Drittstaaten sowie zu Trackingzwecken übermitteln. Es ist auch nicht auszuschliessen, dass diese Drittanbieter diese Daten wiederum zu eigenen Zwecken, die nicht vom Liechtensteinischen Lehrplan gedeckt sind, verwenden. Genau diese Verarbeitung zu eigenen Zwecken durch den Auftragsverarbeiter oder dessen Unterauftragsverarbeiter wird als kritisches Element in einem Auftragsverhältnis gemäss Art. 28 Abs. 3 Bst. a DSGVO gesehen. Eine solche Verarbeitung zu eigenen Zwecken macht den Auftragsverarbeiter zu einem eigenen Verantwortlichen, und er müsste eine eigene Rechtsgrundlage für diese Datenverarbeitung geltend machen können.

Die Rechtsgrundlage zur Datenverarbeitung im Rahmen des Lehrplans beschränkt sich nämlich klar auf die Verarbeitung jener personenbezogenen Daten, die für die Vermittlung der Lehrinhalte als öffentliche Aufgabe im Sinne des Art. 6 Abs. 1 Bst. e DSGVO erforderlich sind. Folglich erfolgen die durch die Beschwerdegegnerin ermöglichte Datenerhebung und die dem ursprünglichen Zweck nicht mehr entsprechende Datenverarbeitung durch die Auftragsverarbeiter und deren Unterauftragsverarbeiter nicht gesetzeskonform und sind der Beschwerdegegnerin als Verantwortliche bzw. «Auftraggeberin» zuzurechnen, da sie bei der Auswahl ihrer Auftragsverarbeiter eine Pflicht trifft, dafür zu sorgen, dass die Verarbeitung der Daten nur auf ihre Weisung erfolgt und nicht zu weiteren, eigenen Zwecken des Auftragsverarbeiters und dessen Unterauftragsverarbeiter.

Ein Beschwerdeführer brachte vor, dass Videokameras in Strassenlaternen zur Gewährleistung der Sicherheit eines Regierungsmitglieds installiert worden seien und öffentlichen Raum erfassten.

Im Fall einer formellen Beschwerde brachte der Beschwerdeführer vor, es seien Videokameras in Strassenlaternen integriert worden, welche der Sicherheit eines Regierungsmitgliedes dienten und öffentlichen Raum erfassten, ebenso wie das Grundstück des Beschwerdeführers. Die Vor-Ort-Begehung ergab jedoch, dass keine Kameras erkennbar waren. Weitere Abklärungen bestätigten, dass weder die Landespolizei noch die Gemeinde Videokameras in Strassenlaternen betreiben. Die Ausführungen der Gemeinde ergaben, dass es sich bei den vermeintlichen Kameras um Sensoren handelt, welche von den Liechtensteinischen Kraftwerken (LKW) zur Steuerung der Strassenlater-

nen genutzt werden. Bei der Vor-Ort-Begehung wurde zudem festgestellt, dass diese Art von Strassenlaternen in mehreren Strassen in Liechtenstein im Einsatz ist. Die Beschwerde war demnach abzuweisen.

5.2.2 Entscheidungen der Beschwerdekommission für Verwaltungsangelegenheiten (VBK)

Im Berichtsjahr entschied die VBK über vier Beschwerden, welche von einer der beiden Verfahrensparteien gegen Verfügungen der DSS eingebracht worden waren. In sämtlichen Fällen bestätigte die VBK die Entscheidungen der DSS.

5.2.3 Beschwerde an den Verwaltungsgerichtshof (VGH)

Die VBK-Entscheidung betreffend eine Videoüberwachung durch eine öffentliche Stelle wurde von letzterer mittlerweile an die übergeordnete Instanz weitergezogen und Beschwerde an den Verwaltungsgerichtshof erhoben.

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.

2022 erhielt die DSS 40 Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO, wovon in 14 Fällen die betroffenen Personen über die Datenschutzverletzung benachrichtigt wurden (Art. 34 DSGVO). Dies bedeutete einen Rückgang zum Vorjahr, in dem 55 Meldungen nach Art. 33 DSGVO erfolgt waren. Allerdings nahmen im Berichtsjahr diejenigen Fälle deutlich zu, in denen die Betroffenen zu informieren waren. Insbesondere diese Frage der Information der Betroffenen erforderte in den meisten Fällen einen grösseren Beratungsaufwand durch die DSS.

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.

Auch die Frage der Notwendigkeit einer Benachrichtigung der betroffenen Personen gemäss Art. 34 DSGVO brachte regelmässig Schwierigkeiten mit sich. Viele Verantwortliche taten sich schwer bei der Beurteilung, ob für die persönlichen Rechte und Freiheiten natürlicher Personen voraussichtlich ein hohes Risiko besteht oder nicht. Die DSS unterstützte die Verantwortlichen deshalb bei der Klärung dieser Frage.

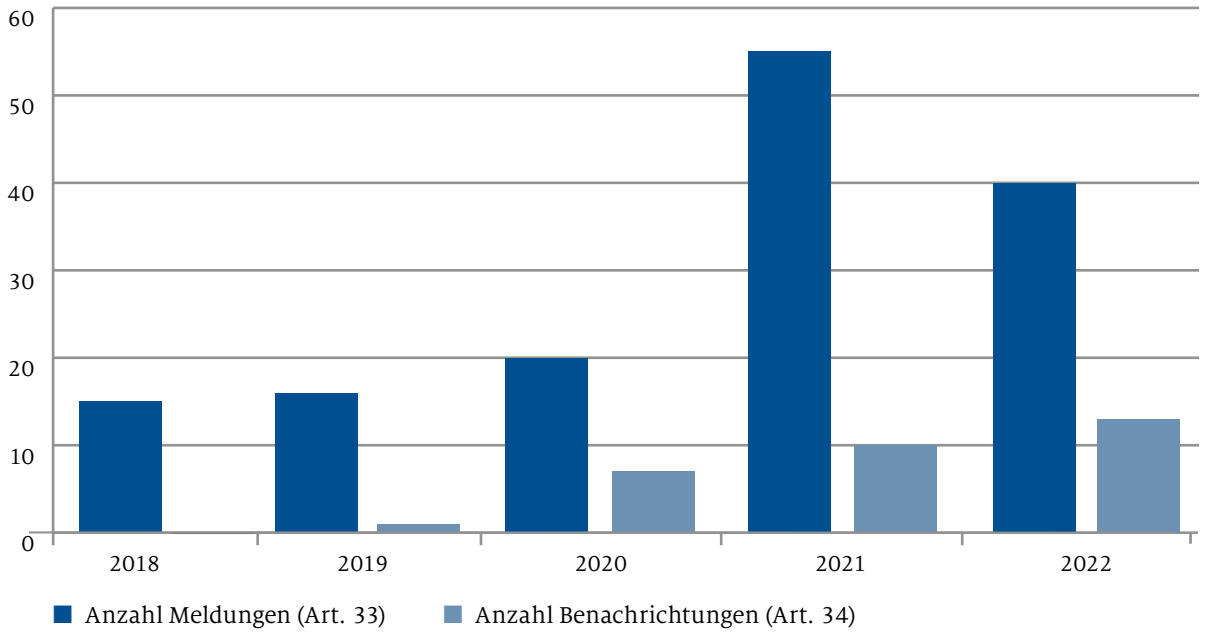


Abbildung 6: Anzahl der gemeldeten Datenschutzverletzungen pro Jahr

«Die DSS forderte, die vom Austausch betroffenen personenbezogenen Daten auf das unbedingt erforderliche Ausmass zu reduzieren sowie mittels technischer und organisatorischer Massnahmen zu gewährleisten, dass die Sicherheit der Daten jederzeit gewährleistet ist.»

6. Mitarbeit in Arbeitsgruppen, Projekten und Kommissionen der Landesverwaltung

6.1 Ratifikation Konvention 108+

Die DSS hat auch im Berichtsjahr wieder 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. Im Berichtsjahr war die DSS erneut in vorbereitende Arbeiten für den entsprechenden Regierungsantrag und den Bericht und Antrag an den Landtag involviert. Die formelle Ratifikation des Änderungsprotokolls durch Liechtenstein wird für 2023 erwartet.

6.2 Datenschutzrechtliche Fragen zum Gesetz über das zentrale Personenregister (ZPRG) – zweite Lesung

Im Rahmen der Vorbereitung auf die zweite Lesung des ZPRG im Landtag musste das Ministerium für Präsidiales und Finanzen mehrere datenschutzrechtliche Fragen beantworten, die von den Landtagsabgeordneten im Laufe der ersten Lesung aufgeworfen worden waren. Es ging vor allem um die Frage der Datenrichtigkeit, die Haftung für unrichtige Daten im Zusammenhang mit dem Grundsatz, dass sich öffentliche Stellen auf die Richtigkeit der Daten im ZPR verlassen können, die Aufbewahrungsfrist für die Protokollierung der Datenverarbeitung, die Rechte der Betroffenen nach Datenschutzrecht (z.B. Information, Berichtigung etc.), die Stelle, bei der diese Betroffenenrechte geltend gemacht werden können, sowie die Löschung von «Falscheinträgen». Die Fragen konnten alle in Kooperation mit dem Ministerium beantwortet werden. Für die Frage der Definition des Begriffs «Datenqualität» wurde von der DSS vorgeschlagen, sich an der Definition der ISO Norm 25012:2008 zu orientieren. Diese bietet für die Definition des Begriffs eine Liste von Kriterien, die erfüllt sein müssen, um eine entsprechende Datenqualität zu gewährleisten, und bietet auch praktische Handlungsempfehlungen zur Erreichung dieses Ziels. Die Antworten fanden schliesslich Eingang in die Stellungnahme der Regierung an den Landtag.

6.3 Datenschutzrechtliche Fragen zum Staatsvertrag mit der Schweiz über Spielersperren

Im Berichtsjahr entschieden Liechtenstein und die Schweiz, dass sie mittels eines Staatsvertrags verhindern wollen, dass gesperrte Personen in einem Casino des jeweils anderen Landes weiterspielen können. Das Abkommen soll einer Stärkung des Schutzes der Spielerinnen und Spieler vor Spielsucht dienen. Die Übermittlung der Spielverbote/-sperren bzw. von deren Aufhebungen soll direkt zwischen den schweizerischen und liechtensteinischen Spielbanken erfolgen. Aus datenschutzrechtlicher Sicht war festzustellen, dass ein solcher Datenaustausch zwischen Liechtenstein und der Schweiz grundsätzlich zulässig ist. Der Staatsvertrag bietet dazu die in Art. 6 Abs. 1 Bst. e DSGVO geforderte gesetzliche Grundlage. Die Grundsatzfrage, ob die Schweizer Casinos bei der Verarbeitung der Daten betreffend die Spielersperren automatisch die DSGVO anzuwenden hätten, konnte die DSS verneinen. Die DSGVO ist von einem Unternehmen in einem Drittstaat nur dann anzuwenden, wenn eine der Bedingungen in Art. 3 Abs. 2 DSGVO erfüllt ist. Das heisst, die Spielbank in der Schweiz bietet ihre Dienstleistungen explizit auch Bürgern im EU/EWR-Raum an oder beobachtet das Verhalten von Bürgern im EU/EWR-Raum. Im vorliegenden Fall geht es aber nicht um ein Angebot an Bürger im EU/EWR-Raum, sondern um einen Datenaustauch zu einem anderen Zweck, nämlich den gesetzlich bzw. staatsvertraglich angeordneten Austausch von Spielersperren. Die Anwendung von Schweizer Recht ist aber insofern unproblematisch, als die Schweiz über einen Angemessenheitsbeschluss der EU-Kommission verfügt. Aus Sicht der DSS wurde zudem angeregt, die vom Austausch betroffenen personenbezogenen Daten auf das unbedingt erforderliche Ausmass zu reduzieren sowie mittels technischer und organisatorischer Massnahmen zu gewährleisten, dass die Sicherheit der Daten jederzeit gewährleistet ist.

6.4 Beratung zu weiteren Gesetzgebungsprozessen

Zusätzlich zu den genannten umfassenden Beratungen beriet die DSS auch diverse weitere Stellen zu Einzelfragen in verschiedenen Gesetzgebungsprozessen.

In Bezug auf das **Gesetz zur Familienhilfe** empfahl die DSS, dass für den Fall, dass bei den Tätigkeiten der Familienhilfe kein ärztliches Personal zum Ein-

satz kommt, im Gesetz spezifiziert werden muss, dass auch das eingesetzte, nicht-ärztliche Personal einer Geheimhaltungspflicht unterliegt. Zudem muss sichergestellt werden, dass alle Mitarbeitenden, die personenbezogene Daten verarbeiten, auch eine eigene Verschwiegenheitsverpflichtung unterzeichnen.

Das Amt für Berufsbildung und Berufsberatung (ABB) ersuchte die DSS um Unterstützung bei der Beantwortung der Frage eines Abgeordneten zu Art. 67 des revidierten BuA zum **Berufsbildungsgesetz** (BBG). Der Abgeordnete stellte die Frage, ob der ämterübergreifende Datenaustausch inskünftig noch möglich sei, da der neue Art. 67 Abs. 4 BBG diesen auf drei Kategorien von Akteuren – das ABB, die beauftragten Bildungsinstitutionen sowie die mit der Durchführung von Prüfungen beauftragten Stellen – begrenze.

Das in Art. 67 Abs. 4 BBG gewählte Verfahren lässt sich aus Sicht der DSS folgendermassen begründen: In Art. 67 Abs. 4 ist explizit ein Abrufverfahren mittels der beim ABB eingesetzten Amtssoftware beschrieben. Beim Abrufverfahren handelt es sich nicht direkt um eine Datenoffenlegung, welche ein aktives Tun seitens des ABB erfordert, sondern vielmehr um einen eigenständig eingerichteten Zugriff für die genannten Stellen. Die Verarbeitung personenbezogener Daten im Abrufverfahren soll nur den drei in Art. 67 Abs. 4 erwähnten Kategorien von Akteuren ermöglicht werden. Es handelt sich bei den drei Kategorien mit Abrufrecht um jene Stellen, die auf die Daten regelmässig zugreifen müssen. Eine Kontaktaufnahme für jeden Einzelfall wäre für diese Stellen wie auch das ABB deshalb mit grossem Aufwand verbunden.

Das Abrufverfahren hat den Vorteil, dass der Zugang zu den Daten vereinfacht und vor allem automatisch eingerichtet wird. Es hat hingegen auch den Nachteil, dass der automatische Zugriff jederzeit möglich ist und somit einer geringeren Kontrolle unterliegt. Um den Schutz der personenbezogenen Daten zu gewährleisten, wurden die Zugriffsberechtigungen im Abrufverfahren entsprechend eingeschränkt. Die Eingrenzung auf die drei Kategorien von Akteuren ist damit auch eine technische bzw. organisatorische Massnahme, um die Daten vor Missbrauch zu schützen und den Zugriff abgestuft nach Erforderlichkeit für andere Behörden und Stellen zu gestalten.

Die Datenoffenlegung für andere Stellen, die nicht unter die drei Kategorien fallen, ist in Art. 67 Abs. 2 geregelt. Für diese anderen Stellen, welche die Daten weniger regelmässig benötigen, ist die Kontaktaufnahme mit dem ABB auch kein solch grosser Aufwand. Art. 67 Abs. 2 ermöglicht damit die angefragte amtsübergreifende Kommunikation. Im Gegensatz zum Abrufverfahren braucht es in den Fällen des Art. 67 Abs. 2 zwar eine direkte Kontaktaufnahme und ein Ersuchen, inklusive Begründung der Erforderlichkeit der Datenoffenlegung. Allerdings nennt Art. 67 Abs. 2 viele Beispiele für begründete Anfragen zur Datenoffenlegung. Diese Beispiele sind nicht abschliessend aufgelistet, darauf verweist das Wort «insbesondere» im Gesetzestext. Es sind also auch weitere Gründe für eine Offenlegung der Daten zu bestimmten Zwecken möglich. Art. 67 Abs. 4 ist damit im Grunde eine technische Erweiterung zur möglichen Datenoffenlegung aus Art. 67 Abs. 2 BBG.

Auch in Bezug auf die Abänderungen des **Statistikgesetzes** und des **Heimatschriftengesetzes,** die **Gesetzesvorlage in Sachen nachrichtenlose Vermögen** sowie den geplanten **Staatsvertrag mit Österreich zur Übernahme von Vollzugsaufgaben im Tabakbereich** stellten sich datenschutzrechtliche Fragen und die DSS wurde hier ebenfalls beratend tätig.

6.5 Fahrradwettbewerb.li

Stellvertretend für die gemeinsam Verantwortlichen (Amt für Hochbau und Raumplanung, Liechtensteinische Industrie- und Handelskammer und Verkehrsclub Liechtenstein) des Projekts «fahrradwettbewerb.li» ersuchte das Amt für Hochbau und Raumplanung die DSS um Unterstützung bei datenschutzrechtlichen Fragen. Radfahrende können sich für den Wettbewerb registrieren und im Aktionszeitraum aufzeichnen, wie viele Wege / Kilometer sie mit dem Fahrrad zurücklegen. Wer im Aktionszeitraum eine je Wettbewerb definierte Schwelle mit dem Fahrrad zurücklegt, kann am Ende einen Preis gewinnen. Hauptthema der Beratung war die Ausgestaltung der datenschutzrechtlichen Beziehungen zwischen den beteiligten Parteien. Mit Unterstützung der DSS konnte ein Vertrag zur gemeinsamen Verantwortlichkeit gemäss Art. 26 DSGVO sowie ein Auftragsverarbeitungsvertrag gemäss Art. 28 DSGVO mit dem Energieinstitut Vorarlberg ausgearbeitet werden. Zudem wurde die Datenschutz-Information gemäss Art. 13 DSGVO für die Besucher der Internetseite sowie die teilnehmenden Personen und die Verarbeitung von deren Daten bei einer Teilnahme an ausgeschriebenen Kampagnen und Wettbewerben vorbereitet.

6.6 VwEG-Kommission

Gemäss Art. 13 des Gesetzes vom 6. Dezember 2018 über das Verzeichnis der wirtschaftlichen Eigentümer inländischer Rechtsträger (VwEG) hat die DSS Einsitz in der VwEG-Kommission. Im Berichtsjahr wurden zwei Anträge gemäss Art. 12 VwEG betreffend die Offenlegung von Daten an Dritte an das Amt für Justiz gestellt. Beide Anträge wurden von der VwEG-

Kommission im Berichtsjahr entschieden. In einem Fall erhob der Antragsteller gegen den negativen Entscheid der VwEG-Kommission eine Beschwerde an die VBK.

«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 2022 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 2022 auf Grundlage des Art. 64 Abs. 1 DSGVO insgesamt **32 Stellungnahmen** zu Vorlagen von nationalen Datenschutz-Aufsichtsbehörden abgegeben. Darunter fielen:

- drei Stellungnahmen zu je einem Entscheidungsentwurf bezüglich der Akkreditierungsanforderungen für eine Stelle zur Überwachung von Verhaltensregeln gemäss Art. 41 DSGVO (Bulgarien, Luxemburg, Slowenien);
- drei Stellungnahmen zu je einem Entscheidungsentwurf bezüglich der Akkreditierungsanforderungen für eine Zertifizierungsstelle gemäss Art. 43 Abs. 3 DSGVO (Bulgarien, Frankreich, Polen);
- eine Stellungnahme zum Entscheidungsentwurf bezüglich der DSGVO – CARPA Zertifizierungskriterien (Luxemburg);
- eine Stellungnahme zu den Zertifizierungskriterien des Europäischen Datenschutzgütesiegels (European Privacy Seal, EuroPriSe) für die Zertifizierung von Verarbeitungsprozessen durch Auftragsverarbeiter (Deutschland);
- eine Stellungnahme zu den Europrivacy Zertifizierungskriterien hinsichtlich ihrer Genehmigung durch den Ausschuss als Europäisches Datenschutzsiegel gemäss Art. 42 Abs. 5 DSGVO;
- 23 Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (ANTOLIN Group; zwei zu Bioclinica Group; Daimler Truck Group; DSV Group; zwei zu Ellucian Group; Fresenius Group; Groupon International Limited; Hilti Group; LEYTON Group; Lundbeck Group; Mercedes-Benz Group; MOL Group; Munich Re Reinsurance Group; Norican Group; zwei zu Piano Group; Ramboll Group; zwei zu Samres Group; zwei zu WEBHELP Group).

Daneben haben der EDSA und der Europäische Datenschutzbeauftragte (EDSB) 2022 auch vier **Gemeinsame Stellungnahmen** erlassen:

- Gemeinsame Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) 2021/953 über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von COVID-19-Impfungen und -Tests sowie der Genesung von einer COVID-19-Infektion (digitales COVID-Zertifikat der EU) mit der Zielsetzung der Erleichterung der Freizügigkeit während der COVID-19-Pandemie;
- Gemeinsame Stellungnahme zum Vorschlag des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für den fairen Zugang zu und die Nutzung von Daten (Data Act);
- Gemeinsame Stellungnahme zum Vorschlag für eine Verordnung über den Europäischen Raum für Gesundheitsdaten;
- Gemeinsame Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern.

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

- Beispiele für die Meldung von Verletzungen des Schutzes personenbezogener Daten, Version 2.0 (EDPB Guidelines 01/2021);
- Verhaltensregeln als Instrument für Übermittlungen, Version 2.0 (EDPB Guidelines 04/2021);
- Anwendung des Artikels 60 DSGVO, Version 1.1 (EDPB Guidelines 02/2022);
- Praktische Anwendung der gütlichen Einigung, Version 2.0 (EDPB Guidelines 06/2022).

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

- Betroffenenrechte – Recht auf Auskunft (EDPB Guidelines 01/2022);
- «Dark Patterns» bei Benutzerschnittstellen von Plattformen Sozialer Medien: Wie man sie erkennt und vermeidet (EDPB Guidelines 03/2022);

- Berechnung von Bussgeldern nach der DSGVO (EDPB Guidelines 04/2022);
- Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung (EDPB Guidelines 05/2022);
- Zertifizierung als Instrument für Übermittlungen (EDPB Guidelines 07/2022);
- Ermittlung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters (EDPB Guidelines 08/2022);
- Meldung von Datenschutzverletzungen nach der DSGVO (EDPB Guidelines 09/2022).

Im Berichtsjahr wurde vom EDSA ausserdem eine **Empfehlung** zu folgendem Thema **in die öffentliche Konsultation gegeben:**

- 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 erwähnt, beteiligt sich die DSS aktiv an der Arbeit des EDSA zur einheitlichen Anwendung der DSGVO im EU/EWR-Raum. Dazu hat die DSS nicht nur im Ausschuss selbst, sondern auch in diversen seiner Arbeitsgruppen (Expert Subgroups, Taskforces) zu ganz unterschiedlichen Themen Einsitz, welche nachfolgend dargestellt werden. Die Mitarbeitenden der DSS haben 2022 an insgesamt 150 Sitzungen des Ausschusses und solcher Arbeitsgruppen teilgenommen.

Die spezielle Arbeitsgruppe des EDSA zu Bussgeldern gemäss DSGVO *(Taskforce Fining)* befasst sich mit der konkreten Berechnung solcher Bussgelder und strebt europaweit eine möglichst einheitliche Herangehensweise an. 2022 wurden nun die offiziellen Leitlinien vom EDSA dazu verabschiedet und in die öffentliche Konsultation gegeben. Die Rückmeldungen daraus wurden soweit möglich eingearbeitet. Gleichzeitig setzte die Task Force ihre Arbeit an einer ergänzenden Tabelle zu den Leitlinien fort. Darin werden die Ausführungen und Berechnungsvorgaben auch noch tabellarisch dargestellt, womit einem entsprechenden Bedürfnis nachgekommen wird. Die Arbeiten sind schon weit fortgeschritten, sodass die Leitlinien einschliesslich der Tabelle 2023 vom EDSA final verabschiedet werden können.

Diejenige 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 mehrerer Verfahren im Rahmen des Streitbeilegungsmechanismus gemäss Art. 65 DSGVO beschäftigt. Zahlreiche betroffene Aufsichtsbehörden hatten massgeblichen und begründeten Einspruch gegen die Beschlussentwürfe der federführenden Aufsichtsbehörde eingelegt, dem sich diese jedoch nicht angeschlossen bzw. den diese abgelehnt hatte. Der in solchen Fällen erforderliche verbindliche Beschluss des EDSA zur Streitbeilegung wurde von der Arbeitsgruppe für fünf Verfahren vorbereitet.

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 im Rahmen der speziellen *Taskforce 101* und *Cookie Banner Taskforce* fortgeführt. Erstere befasst sich mit der einheitlichen Beurteilung der 101 Beschwerden der Organisation *Non of Your Business* (noyb) des Datenschutz-Aktivisten Max Schrems zum Einsatz von Google Analytics und Facebook Pixel auf Webseiten. Die Beschwerden zu Google Analytics wurden dabei im Berichtsjahr von den europäischen Behörden (sofern zulässig) gutgeheissen und der Einsatz von Google Analytics in der vorliegenden Form als nicht rechtskonform beurteilt. Die Verfahren zum Einsatz von Facebook Pixel sind noch anhängig. Die *Cookie Banner Taskforce* bearbeitet diverse Fragen rund um die rechtlich zulässige oder unzulässige Gestaltung von Cookie-Bannern. Sie wird ihren abschliessenden Bericht 2023 publizieren. Wertvoll aus Sicht der DSS war auch wieder der im Rahmen der Arbeitsgruppe regelmässig geführte Austausch über grössere laufende Verfahren oder wichtige Entscheidungen der Aufsichtsbehörden.

Ende April fand zudem ein Treffen aller Leiterinnen und Leiter der EU/EWR-Datenschutzbehörden in Wien statt, um Massnahmen zur Verbesserung der Durchsetzung des Datenschutzes und der DSGVO in allen Mitgliedsstaaten zu beschliessen. Einerseits wurde die Wichtigkeit bereits aufgegleister Projekte wie des *Support Pool of Experts*, auf welchen die Behörden bei Bedarf zugreifen können, oder des *Coordinated Enforcement Frameworks*, auf welches im nächsten Abschnitt noch weiter eingegangen wird, betont. Andererseits wurden auch zusätzliche Massnahmen beschlossen, wie etwa eine Verbesserung der Kommunikation unter den Behörden, eine Vereinfachung der Behandlung grenzüberschreitender Fälle oder die Priorisierung strategisch wichtiger Fälle, an deren Beurteilung mehrere Aufsichtsbehörden gemeinsam arbeiten sollen. Dies nicht zuletzt, um aufwändige Streitbeilegungsverfahren von Anfang an zu vermeiden. Die Bearbeitung erster solch strategisch wichtiger Fälle hat bereits im zweiten Halbjahr 2022 begonnen.

Die mit der einheitlichen Durchsetzung der DSGVO befasste Arbeitsgruppe hat im Vorjahr auch das erwähnte *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 und Aktivitäten) als auch gemeinsam lancierte, europaweite Kontrollen in Betracht. Jede Aufsichtsbehörde kann dabei frei entscheiden, ob sie sich an einer solchen koordinierten Aktion beteiligen will und welches Mittel sie dafür einsetzen möchte.

Die erste solche *Coordinated Action* wurde 2022 durchgeführt und hat sich mit der Nutzung von Cloud-basierten Services durch öffentliche Stellen befasst. Die DSS hat sich daran ebenfalls beteiligt und mittels eines umfangreichen Fragebogens beim Amt für Informatik (AI), als zentralem Beschaffungsorgan für öffentliche Stellen in Liechtenstein, Informationen darüber erhoben, wie Cloud-basierte Services derzeit für öffentliche Stellen ausgewählt, beschafft und genutzt werden und wie dabei den datenschutzrechtlichen Vorgaben nachgekommen wird. Die Antworten hat die DSS in einem nationalen Bericht zusammengefasst, der in einem aggregierten Abschlussbericht auf europäischer Ebene anfangs 2023 vom EDSA veröffentlicht wird. Durch die im Rahmen dieser koordinierten Aktion gewonnenen Erkenntnisse kann die DSS das AI künftig noch gezielter bei entsprechenden Projekten unterstützen und gleichzeitig sicherstellen, dass von Anbietern Cloud-basierter Services in Liechtenstein die gleichen Konditionen eingefordert werden können wie auch in anderen europäischen Ländern.

Für 2023 wurde bereits eine neue *Coordinated Action* initiiert, welche sich mit der Ernennung und der Rolle von Datenschutzbeauftragten befasst.

In der Arbeitsgruppe, welche sich mit der Zusammenarbeit der Aufsichtsbehörden befasst *(Cooperation Subgroup)*, wurde im Berichtsjahr zunächst eine Toolbox für datenschutzrechtliche Garantien bei der Zusammenarbeit mit Datenschutz-Aufsichtsbehörden in Drittstaaten erarbeitet. Sodann wurden die verschiedenen Teile der Leitlinien zum Kooperationsverfahren bei grenzüberschreitenden Beschwerden gemäss Art. 60 DSGVO in einem Dokument konsolidiert und vom EDSA final verabschiedet. Diese Leitlinien schaffen ein harmonisiertes europäisches Verfahren für grenzüberschreitende Fälle, welches dennoch Raum für die involvierten nationalen Verfahrensrechte lässt. Und schliesslich wurden die Leitlinien zur gütlichen Streitbeilegung im Rahmen grenzüberschreitender Verfahren fertiggestellt und verabschiedet. Als Folge des Wien-Treffens der Leiterinnen und Leiter der europäischen Datenschutzbehörden wurde ausserdem die Arbeit an einer Guidance für die Vereinfachung der Behandlung grenzüberschreitender Fälle aufgenommen. Ebenfalls begonnen wurde mit den Arbeiten an Leitlinien zu den datenschutzrechtlich relevanten Teilen der europäischen CSAM-Verordnung sowie zum Art. 61 DSGVO. Darüber hinaus gab es erste Abklärungen für eine gemeinsame europäische Datenbank für Vertreter von Organisationen aus Drittstaaten sowie für ein gemeinsames europäisches Beschwerdeformular für betroffene Personen.

Die thematische Arbeitsgruppe zu Finanzangelegenheiten des EDSA *(Financial Matters Subgroup)* hat im Berichtsjahr einen aktiven Austausch mit der Europäischen Zentralbank zum voranschreitenden Projekt der Einführung eines Digitalen Euros geführt. Ausserdem hat die Arbeitsgruppe mehrere Stellungnahmen an die Kommission abgegeben zur Revision der Gesetzgebung über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung. Darüber hinaus hat sie wiederum diverse kleinere Beiträge und Stellungnahmen zu Themen wie PSD2, FATCA, Mobile Payments, Informations-Dienstleistern im Bereich der Geldwäschereibekämpfung, Open Finance, zur Revision der Konsumkreditrichtlinie oder zum internationalen Datenaustausch für die FATF sowie für die EIOPA, EBA und ESMA erarbeitet. Viele dieser Arbeiten werden auch 2023 fortgeführt. Die DSS stand bei einzelnen Themen im Berichtsjahr auch in Kontakt mit der FMA, um sich gegenseitig zu informieren und auszutauschen.

Die Arbeitsgruppe zu Fragen bezüglich Datenübermittlungen in Drittstaaten *(International Transfer Subgroup)* hat im Berichtsjahr die Arbeiten an der Zertifizierung als geeignete Garantie für internationale Datentransfers wie auch an der Richtlinie zur entsprechenden Nutzung von Verhaltensregeln (Code of Conduct) weitergeführt. Letztere wurde nach der öffentlichen Konsultation überarbeitet und endgültig abgeschlossen. Wohingegen die Richtlinie über Zertifizierungen als geeignete Garantien im Berichtsjahr in die öffentliche Konsultation ging, die finale Überarbeitung jedoch noch nicht abgeschlossen werden konnte. Dies ist im Folgejahr zu erwarten. Nachdem die schon seit Jahren diskutierte, genaue Definition eines internationalen Datentransfers im Jahr 2022 abgeschlossen und in die öffentliche Konsultation gegeben wurde, gaben die daraufhin eingegangenen Anmerkungen und Rückmeldungen nochmals Anlass zu

intensiven Diskussionen und einer umfassenden Überarbeitung der Richtlinie über das Zusammenspiel von Artikel 3 und Kapitel 5 DSGVO zum internationalen Datentransfer, welche das gesamte Berichtsjahr andauerten. Dies veranschaulicht, wie relevant, aber auch komplex sich die vorgeblich einfache Definition eines internationalen Datenverkehrs herausstellt. Ein finaler Abschluss ist im Folgejahr zu erwarten.

Die schon seit zwei Jahren laufende, umfassende Überarbeitung der Hilfestellung für die BCR-Verfahren (Working-Paper 256) für sogenannte «Controller BCR» (Verbindliche interne Datenschutzvorschriften für Verantwortliche) konnte im Berichtsjahr abgeschlossen und in die öffentliche Konsultation gegeben werden. Dies ist ein beträchtlicher Schritt im Bereich der Hilfestellung zur Ausarbeitung von BCR. In Bezug auf die konkrete Genehmigungspraxis durch die Aufsichtsbehörden stellte sich jedoch die Frage, ab wann diese neuen Regeln und Genehmigungsvoraussetzungen von allen Aufsichtsbehörden einheitlich berücksichtigt werden sollen. Ein BCR-Genehmigungsverfahren dauert jeweils mehrere Jahre. Bereits laufende Verfahren stützen sich dabei noch auf die alten Regeln und Voraussetzungen, müssen jedoch früher oder später ohnehin auf die neuen angepasst werden. Die Arbeitsgruppe hat sich nun darauf geeinigt, ab welchem Verfahrensstand die neuen Standards umzusetzen sind und dass alle anderen dies in der ersten jährlichen Überprüfung und Aktualisierung der BCR angehen müssen.

Die CEH-Arbeitsgruppe *(CEH Expert Subgroup),* eine Kurzbezeichnung für Compliance, E-Government und Health, befasst sich mit Themen im Zusammenhang mit Zertifizierung und Akkreditierung sowie E-Government und Gesundheit. Betreffend Zertifizierung und Akkreditierung prüfte die CEH-Arbeitsgruppe in ihren Sitzungen im Berichtsjahr die Akkreditierungskriterien für Überwachungsstellen nach Art. 41 DSGVO und die Akkreditierungskriterien für Zertifizierungsstellen nach Art. 43 DSGVO von verschiedenen Mitgliedstaaten, zu denen der EDSA nachfolgend eine Stellungnahme verfassen sollte. Ebenfalls befasste sich die Arbeitsgruppe mit den Zertifizierungskriterien des europäischen Datenschutzgütesiegels «EuroPriSe», welche dem EDSA von der Datenschutzbehörde Nordrhein-Westfalen zur Stellungnahme gemäss Art. 64 Abs. 1 Bst. c DSGVO unterbreitet worden waren. Des Weiteren widmete sich die Arbeitsgruppe den Zertifizierungskriterien des europäischen Datenschutzgütesiegels «Europrivacy», welche seitens der luxemburgischen Datenschutzaufsichtsbehörde beim EDSA zur Genehmigung gemäss Art. 70 Abs. 1 Bst. o DSGVO eingereicht worden waren. Dieses Zertifizierungssystem war im Rahmen des europäischen Forschungsrahmenprogramms «Horizon» 2020 entwickelt worden. Es ist für eine weitgespannte Palette von Datenverarbeitungstätigkeiten nutzbar, insbesondere auch für die Anwendung neuer Technologien wie künstlicher Intelligenz, Internet der Dinge, Blockchain, automatisierte Fahrzeuge etc.

Weiter prüfte die CEH-Arbeitsgruppe auch die datenschutzrechtlichen Implikationen des neuen europäischen «Data Act», der als Ergänzung des «Data Governance Act» dienen soll. Der Data Act stellt ebenfalls eine wichtige Säule der europäischen Datenstrategie dar und sorgt für Regeln bei der Nutzung von Daten, welche von Geräten des Internets der Dinge (IoT) generiert werden. Der Data Act soll hierbei gewährleisten, dass die Weitergabe, Speicherung und Verarbeitung solcher Daten gemäss den europäischen Rechtsvorschriften erfolgt.

Im Gesundheitsbereich, dem zweiten grossen Themenbereich der CEH-Arbeitsgruppe, befasste sich diese im Berichtsjahr mit dem Regulierungsvorschlag der Europäischen Kommission zu einem europäischen Gesundheitsdatenraum (European Health Data Space, EHDS). Mit dem EHDS wird ein gemeinsamer europäischer Raum für Gesundheitsdaten etabliert, welcher die verschiedenen Bereiche von Gesundheitsdaten europaweit zusammenführt. Der EHDS soll es dabei einerseits natürlichen Personen erlauben, jederzeit auf ihre Daten zugreifen und diese kontrollieren zu können, und es andererseits auch medizinischem Personal ermöglichen, die Erbringung ihrer Leistungen in punkto Diagnostik und Behandlung zu optimieren. Überdies soll der EHDS im Bereich der Forschung genutzt werden können. Und schliesslich soll der EHDS auch für politische Entscheidungsträger zum Zwecke regulatorischer Aktivitäten nutzbar sein (Sekundärnutzung).

Die Arbeitsgruppe zu technologischen Themen *(Technology Expert Subgroup)* befasste sich wie im Jahr 2021 mit einem breiten Spektrum an Fragestellungen und entwarf mehrere Leitlinien, Empfehlungen sowie Stellungnahmen des EDSA. Am 11. Mai 2022 veröffentlichte die Europäische Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern. Als Reaktion auf diesen Vorschlag wurde im Juli 2022 die Gemeinsame Stellungnahme des EDSA und des Europäischen Datenschutzbeauftragten (EDSB) veröffentlicht, welche von der Arbeitsgruppe vorbereitet wurde. Zusammengefasst äussern EDSA und EDSB ernsthafte Bedenken hinsichtlich der Verhältnismässigkeit der geplanten

Eingriffe in bzw. Einschränkungen der Grundrechte auf Schutz der Privatsphäre und der personenbezogenen Daten. In diesem Zusammenhang werden derzeit von der Arbeitsgruppe auch Leitlinien über den Einsatz von Technologien zur Aufdeckung und Meldung von sexuellem Kindesmissbrauch im Internet ausgearbeitet. Die Verabschiedung dieser Leitlinien durch den Ausschuss wird innerhalb des ersten Halbjahres 2023 erwartet.

Sowohl die Leitlinie zur Anonymisierung und Pseudonymisierung als auch die Leitlinie zum Thema Blockchain befinden sich nach wie vor in Ausarbeitung. Aufgrund des Umfangs der Leitlinie zur Anonymisierung und Pseudonymisierung wurde entschieden, zwei separate Leitlinien zu verfassen und diese jeweils mit Fallbeispielen anzureichern. Die Arbeit an diesen beiden Dokumenten ist mittlerweile schon sehr weit fortgeschritten. Mit der Verabschiedung durch den Ausschuss ist deshalb noch im ersten Halbjahr 2023 zu rechnen. Weitere Tätigkeiten der Arbeitsgruppe im Berichtsjahr betrafen die Aktualisierung der Leitlinien zur Meldung von Datenschutzverletzungen, den Austausch mit weiteren Behörden sowie den Informationsaustausch zwischen verschiedenen Arbeitsgruppen des EDSA, um nur einige Beispiele zu nennen.

Die Arbeitsgruppe zu Sozialen Medien *(Social Media Subgroup)* fokussierte sich 2022 auf die Fertigstellung der Leitlinien zum Thema Benutzerschnittstellen-Design bei Plattformen Sozialer Medien. Die Version 1.0 dieser Leitlinie wurde im März 2022 verabschiedet. Aufgrund mehrerer Rückmeldungen in der öffentlichen Konsultationsphase wurde eine Version 2.0 erarbeitet, deren Annahme durch den Ausschuss für Anfang 2023 erwartet wird. Am auffälligsten an der Version 2.0 ist sicherlich die Änderung des Begriffs «dark patterns» zu «deceptive design patterns», um eine umfassendere und beschreibendere Sprache zu verwenden. Zusätzlich wurde mit der Ergänzung von zwei Anhängen versucht, die praktische Umsetzung der Leitlinie verständlicher darzulegen. Darüber hinaus befindet sich auch die Leitlinie für die Nutzung Sozialer Medien durch öffentliche Einrichtungen nach wie vor in Ausarbeitung durch die Arbeitsgruppe.

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.

Die BTLE-Arbeitsgruppe *(BTLE Expert Subgroup),* eine Kurzbezeichnung für Border Travel und Law Enforcement, hat zur Aufgabe, die gesetzgeberischen Entwicklungen in den Bereichen Polizei, Grenzverkehr und Strafjustiz zu verfolgen. Die Arbeitsgruppe hat im Berichtsjahr in dieser Hinsicht den Entwurf eines EDSA-Schreibens für den LIBE-Ausschuss zum zweiten Zusatzprotokoll zum Übereinkommen über Computerkriminalität (Budapester Übereinkommen) verfasst, der vom Ausschuss angenommen wurde. Darüber hinaus verfasste die Arbeitsgruppe je ein EDSA-Antwortschreiben auf die Frage eines Europaabgeordneten bezüglich des angeblichen Einsatzes von Spähsoftware durch öffentliche Behörden in Ungarn (Pegasus-Affäre) sowie auf die Frage einer Europaabgeordneten betreffend Fluggastdatensätze. Weiters wurden im Berichtsjahr die Ausarbeitung von Leitlinien zu Art. 37 LED (Datenübermittlung vorbehaltlich geeigneter Garantien) sowie die Ausarbeitung von Leitlinien zu Art. 48 DSGVO bezüglich an Empfänger im EU/EWR-Raum gerichtete Auskunftsersuchen aus Drittländern für Zwecke der Strafverfolgung und der nationalen Sicherheit aufgenommen. Und schliesslich verfasste die Arbeitsgruppe auch Leitlinien für den Einsatz einer Gesichtserkennungstechnologie im Bereich (der Strafverfolgung) von Polizei und Justiz, welche im Berichtsjahr vom Ausschuss angenommen und in die öffentliche Konsultation gegeben wurden.

7.1.2 Gegenseitige Amtshilfe

Die DSGVO erfordert jedoch nicht nur eine Zusammenarbeit der europäischen Datenschutz-Aufsichtsbehörden im bzw. mit dem EDSA, sondern 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 beantwortete im Berichtsjahr 78 Anfragen von anderen europäischen Datenschutzaufsichtsbehörden, was im Vergleich zu den im Vorjahr beantworteten 75 Anfragen eine minimale 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: Datentransfer in ein Drittland, rechtmässige Verwendung von biometrischen Daten, Verwendung von Statusanzeigen von

Kommunikationsdiensten im Beschäftigtenbereich, Direktwerbung (b2b), Anbieter von online-Bezahldiensten oder auch online-Glücksspielen, Videoüberwachungen im öffentlichen Bereich oder auch in Personenkraftfahrzeugen sowie in Altenheimen.

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 Europarat

Die DSS hat im Berichtsjahr an der 43. Versammlung des Beratenden Ausschusses des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) des Europarats teilgenommen. Die Veranstaltung konnte im Herbst zum ersten Mal wieder vor Ort in Strassburg durchgeführt werden. Die Verschiebung der Versammlung von Juni auf November war darauf zurückzuführen, dass im Frühjahr noch nicht formell geklärt war, wie die weitere Beteiligung der russischen Delegation an der Konvention 108 aussehen würde, nachdem Russland zuvor aufgrund des Angriffskrieges auf die Ukraine als Mitglied des Europarats ausgeschlossen worden war.

Der Beratende Ausschuss der Konvention 108 hat im Berichtsjahr Leitlinien zur «Digital Identity» verabschiedet und seine Geschäftsordnung (Rules of Procedure) bezüglich der Modalitäten von Russlands Mitgliedschaft in der Konvention 108 angepasst. Im Übrigen bestand die Hauptarbeit des Beratenden Ausschusses im Berichtsjahr weiterhin in der Erarbeitung von Leitlinien zum Thema zwischenstaatlicher Informationsaustausch zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung sowie zu Steuerzwecken, sowie im Verfassen von Standardvertragsklauseln für grenzüberschreitende Datentransfers. Die Ergebnisse dieser Arbeiten können auch zu künftigen Handlungsempfehlungen, Leitlinien, Resolutionen oder Erklärungen 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. Der Beratende Ausschuss hat sich deshalb im Berichtsjahr auch mit dem angestrebten Inkrafttreten des Änderungsprotokolls sowie der Auslegung von Art. 11 der modernisierten Konvention 108 befasst, welcher die verschiedenen Ausnahmen regelt. Die DSS unterstützt das Amt für Auswärtige Angelegenheiten beim Ratifikationsprozess des Änderungsprotokolls durch Liechtenstein. Im Berichtsjahr war die DSS deshalb weiter massgeblich in die Vorbereitung des Regierungsantrags und des Berichts und Antrags an den Landtag involviert. Die formelle Ratifikation des Änderungsprotokolls durch Liechtenstein wird für 2023 erwartet.

«Datenschutzaufsicht und Verantwortliche oder Auftragsverarbeiter sind keine Gegenspieler.»

8. Schlussbemerkung und Ausblick

Im Hinblick auf die Zukunft stehen wir auch am Ende des Berichtsjahres erneut vor einer Reihe von Herausforderungen im Bereich des Datenschutzes. Einer der wichtigsten Aspekte wird weiterhin die Umsetzung der DSGVO im Alltag der öffentlichen und privaten Stellen sein, denn es zeigte sich im Berichtsjahr erneut, dass selbst bei der Umsetzung der einfachsten Grundsätze noch lange kein Niveau erzielt wurde, das der Intention des Gesetzgebers entspricht. Aus diesem Grund plant die DSS im Folgejahr wieder Workshops durchzuführen, die sich ganz grundlegenden Themen wie einer Datenschutzerklärung für Internetseiten widmen.

Ein weiteres wichtiges Thema wird die Sicherheit von personenbezogenen Daten sein. Hierbei gilt es, angemessene Sicherheitsmassnahmen zu ergreifen, um einen Missbrauch oder eine unbefugte Weitergabe von Daten zu verhindern. Neue Technologien und Trends wie Cloud Computing, Big Data und das Internet der Dinge veranlassen Bürgerinnen und Bürger zunehmend, sich mit diesbezüglichen Fragen und Sorgen an die DSS zu wenden. Mit der wachsenden Anzahl von Daten steigt auch das Risiko von Cyberangriffen und Datenmissbrauch, was schwerwiegende Folgen für betroffene Personen haben kann. Die Verarbeitung personenbezogener Daten birgt auch das Risiko von Identitätsdiebstahl, Finanzbetrug und anderen Formen von Missbrauch. Darüber hinaus können Verletzungen des Datenschutzes das Vertrauen der Öffentlichkeit in Unternehmen, Organisationen und Behörden beeinträchtigen, was zu einem erheblichen Imageverlust führen kann. Daher ist es von grosser Bedeutung, dass angemessene Sicherheitsmassnahmen ergriffen werden, um personenbezogene Daten zu schützen und das Vertrauen der Öffentlichkeit in den Datenschutz zu erhalten. Diese Fragen zu organisatorischen und technischen Massnahmen nehmen in der Beratung, aber auch in den Beschwerden stark zu und erfordern auch künftig ein starkes Engagement der DSS.

Schliesslich wird die Zusammenarbeit mit anderen Datenschutzbehörden in Europa, aber auch weltweit von zentraler Bedeutung sein. Nur durch eine enge Zusammenarbeit können wir sicherstellen, dass die Datenschutzstandards weltweit harmonisiert werden und ein angemessener Schutz für personenbezogene Daten gewährleistet wird.

Datenschutzaufsicht und Verantwortliche oder Auftragsverarbeiter sind keine Gegenspieler. Dieser Grundsatz soll auch künftig die Arbeit der DSS leiten und in den Veranstaltungen, Öffentlichkeitsarbeit, Beratungen und auch in aufsichtsrechtlichen Verfahren zum Ausdruck gebracht werden.

Datenschutzstelle Fürstentum Liechtenstein
Städtle 38
Postfach 684
FL-9490 Vaduz

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