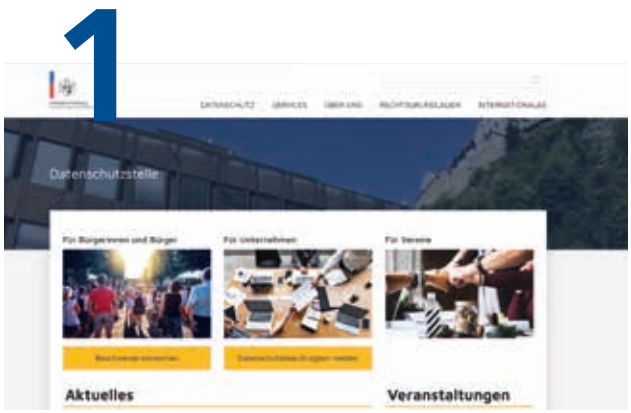
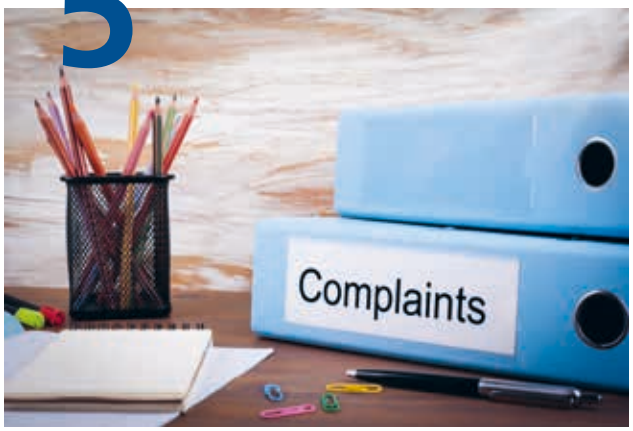
DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht Datenschutzstelle
Fürstentum Liechtenstein

Tätigkeitsbericht 2020

Inhaltsverzeichnis





Impressum

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

Vorwort

Das Berichtsjahr 2020 war kein Jahr wie jedes andere. Die Corona-Pandemie prägte den Alltag der Bürgerinnen und Bürger, der Unternehmen und öffentlichen Einrichtungen weitreichend. Kaum ein Lebensbereich war nicht von der Pandemie und den Massnahmen zu ihrer Bekämpfung betroffen. Mit diesem Tätigkeitsbericht blickt die Datenschutzstelle (DSS) auf dieses turbulente Jahr zurück.

Die Corona-Pandemie hat das Arbeiten in- und ausserhalb der DSS stark verändert. Zahlreiche Fragen und Unsicherheiten vom Wechsel des Arbeitsortes ins Home-Office prägten vor allem das erste Halbjahr und die Anfragen und Beratungen durch die DSS. Videokonferenzen wurden zum Alltag und warfen Fragen auf. Die Kontaktnachverfolgung von möglichen Covid-19-Infizierten mit Handydaten gab Anlass zur Hoffnung bei den Gesundheitsbehörden, verursachte aber auch Unbehagen bei Betroffenen. Die Überlegung, Gästelisten in der Gastronomie verpflichtend einzuführen, führte zu Kopfschütteln bei Wirten und Gästen. Und damit seien nur wenige Beispiele genannt.

Daten schienen für viele gerade in der ersten Zeit der Pandemie-Bekämpfung als Wundermittel und die Versuche, mittels Datensammlung und -verwertung die Pandemie in den Griff zu bekommen, nahmen rasant zu. Der Datenschutz hatte hier eine herausfordernde Bewährungsprobe zu meistern. Und meines Erachtens hat er diese auch tatsächlich recht erfolgreich bestanden. Die Entscheidungen der europäischen Datenschutz-Aufsichtsbehörden sowie des Europäischen Datenschutzausschusses machten zum einen deutlich, dass der Datenschutz keinesfalls einer effektiven und zielführenden Bekämpfung der Pandemie im Wege steht, dass aber andererseits trotz des hohen Zieles die Achtung der Privatsphäre und der Schutz der Persönlichkeit bzw. der personenbezogenen Daten der Bürgerinnen und Bürger nicht ausser Acht gelassen werden dürfen. Datenschutz ist ein Grundrecht und verdient auch in schwierigen Zeiten einen besonderen Schutz. Die Grundprinzipien der Datenschutz-Grundverordnung (DSGVO) gaben für die Abwägung und die Suche nach einem Gleichgewicht zwischen Datennutzung zur Bekämpfung der Pandemie und Schutz der Privatsphäre klare Leitlinien vor und sorgten mit ihrem europaweit einheitlichen Standard für (zumindest annähernd) klare Grenzen. Auch schien die Einhaltung des Datenschutzes die gesellschaftliche Akzeptanz der Tracing Apps oder ähnlicher Instrumente zu stärken, sorgte dieser doch dafür, dass so viel wie nötig, doch vor allem so wenig wie möglich in die Grundrechte eingegriffen wird.

Dr. Marie-Louise Gächter, Leiterin Datenschutzstelle

Um das Vertrauen ging es auch im Home-Office. Eine kompromisslose und wasserdichte Datensicherheit ist Grundvoraussetzung für das Vertrauen der Bürgerinnen und Bürger oder Konsumenten, wenn ihre Daten neuerdings nicht mehr in gesicherten Bürogebäuden, sondern in den Privatwohnungen der Mitarbeitenden verarbeitet werden. Die Zeit für die Vorbereitung des Wechsels ins Home-Office war kurz. Was im Normalfall jahrelanger Vorbereitung und Planung bedarf, musste in kürzester Zeit bewerkstelligt werden. Dazu kam, dass das Urteil des Europäischen Gerichtshofs (EuGH) im Juli 2020 in der Rechtssache «Schrems II» den Datentransfer in die USA vor eine grosse Hürde stellte. Und dies just zu einer Zeit, als viele europäischen Institutionen auf der Suche nach digitalen Lösungen für das Home-Office waren und dabei der Einfachheit halber häufig auf Anbieter aus Übersee zurückgriffen, deren Lösungen schnell und unkompliziert einsatzbereit waren.

Diese und zahllose weitere Fragestellungen beschäftigten im Berichtsjahr neben vielen anderen

betroffenen Stellen auch die Datenschutz-Aufsichtsbehörden. Ganz allgemein und unabhängig von den Antworten auf die vielzähligen Fragen lässt sich vor allem ein Fazit ziehen: Die DSGVO hat sich auch in der aussergewöhnlichen Situation der Corona-Pandemie erneut bewährt, genauso wie ihre ehrgeizige Zielsetzung, eine Harmonisierung des Datenschutzes in den EWR-Staaten zu erreichen. Denn an die 30 datenschutzrechtliche Einzellösungen in Europa wären für die vielen grenzüberschreitend tätigen Unternehmen eine (zu) grosse Hürde und in der Kürze der Zeit wohl auch kaum zu befolgen gewesen.

Vaduz, im April 2021

Einleitung

Auch Liechtenstein blieb von den im Vorwort genannten Herausforderungen nicht verschont. Corona-Apps, Covid-19-Forschungsprojekte, Digitalisierung im Kontext von Home-Office oder Home-Schooling, Beschäftigten-Datenschutz im Home-Office, Datenschutz-Konformität von Videokonferenz-Systemen wie Microsoft Teams, Google Meet, Cisco Webex und Zoom prägten die Fragestellungen, die die DSS seit Beginn der Corona-Pandemie von privaten und öffentlichen Stellen, aber auch von zahlreichen Bürgerinnen und Bürgern erhielt. Gerade letztere wandten sich häufiger als im Vorjahr mit Anfragen, aber auch mit Hinweisen auf mögliche Datenschutzverletzungen und Beschwerden an die DSS. Dies zeigt deutlich, dass die Menschen in Liechtenstein zunehmend bereit sind, ihre Rechte und Freiheiten zum Schutz ihrer Privatsphäre auch tatsächlich durchzusetzen und sich dafür an die zuständige Aufsichtsbehörde zu wenden.

Die von der DSS durchgeführten Untersuchungen machten auch im Berichtsjahr wieder deutlich, dass öffentliche und private Institutionen aus unterschiedlichsten Gründen die Rechte und Freiheiten der betroffenen Personen missachten. Die Verletzungen des Datenschutzes sind neben bewusstem Missbrauch oft auch Resultat fehlenden Wissens, von Sorglosigkeit, Unvermögen oder schlechter Beratung. Keine dieser Begründungen vermag allerdings eine Verletzung der Rechte der Betroffenen zu rechtfertigen. Für die Arbeit der DSS bedeutet dies, dass es nach wie vor zweier Elemente zur Gewährleistung von Datenschutz, des in der digitalen Welt zentralen Grundrechts für die Menschen, bedarf: Neben der Untersuchung von Beschwerdefällen braucht es vor allem auch die präventive Beratung und Information der Verantwortlichen. Durch die Einschränkung der Veranstaltungsmöglichkeiten aufgrund der Covid-19-Massnahmen kam diese Präventionsarbeit 2020 bedauerlicherweise zu kurz und es konnten nicht ganz so viele Verantwortliche erreicht werden wie gewünscht.

Nichtsdestotrotz war das Berichtsjahr ein sehr aktives Jahr für die DSS, das nicht nur durch die Covid-19-Pandemie und die daraus resultierenden Datenschutzfragen, sondern auch die ungeheure Dynamik der Entwicklung digitaler Technologien zahlreiche Herausforderungen an das Team der DSS stellte. Beide Bereiche machten dabei jedoch eines deutlich: Weder der Gesundheitsschutz noch die technologische Entwicklung stehen mit dem Datenschutz in einem Entweder-Oder-Verhältnis. Keiner sollte dem anderen untergeordnet werden, sondern auf den jeweiligen konkreten Fall bezogen seinen Platz einnehmen dürfen und in Einvernehmen nebeneinander bestehen können bzw. zu einem Miteinander finden. Zugegebenermassen können diese Abwägungen bisweilen mit Aufwand verbunden sein und nicht immer in der einfachsten Lösung resultieren. Auf langfristige Sicht sind die so gefundenen aber die besten Lösungen, da sie sowohl einen Vertrauensverlust bei den betroffenen Personen als auch langwierige Beschwerdeverfahren verhindern. Die DSS sah es deshalb auch im Berichtsjahr als ihre vorrangige Pflicht an, die verschiedenen Akteure bei der Lösungssuche zu unterstützen und so für einen Ausgleich zwischen der Projektrealisierung durch die Verantwortlichen und dem Schutz der betroffenen Personen zu sorgen.

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

1. Öffentlichkeitsarbeit

Datenschutz lässt sich nicht nur aus Lehrbüchern oder Kommentaren lernen und auch ein alleiniger Blick in den Gesetzestext garantiert nicht eine perfekte praktische Umsetzung der datenschutzrechtlichen Vorgaben. Ohne eine aktive Informations- bzw. Wissensvermittlung seitens der Aufsichtsbehörde wird Datenschutz nicht die Rolle in den öffentlichen und privaten Stellen spielen können, die ihm der Gesetzgeber zugedacht hat.

Für die Vermittlung von Fachinformationen nutzt die DSS vor allem vier Kanäle: Veranstaltungen und Vorträge, Newsletter, ihre Internetseite und individuelle Beratungen. Insbesondere das Zusammenwirken der genannten Kommunikationskanäle ermöglicht es, dass eine sehr grosse Zahl an Adressaten erreicht werden kann. Bedauerlicherweise mussten allerdings zahlreiche Veranstaltungen im Berichtsjahr aufgrund der Covid-19-Beschränkungen abgesagt und Gesprächsrunden auf kleine Kreise beschränkt werden. In manchen Fällen war ein Ausweichen auf Online-Kanäle möglich. Aus diesem Grund konnte die Öffentlichkeitsarbeit im Berichtsjahr jedoch nicht ganz in dem Umfang durchgeführt werden wie geplant.

1.1 Veranstaltungen

Die grösste Veranstaltung im Berichtsjahr war der Datenschutztag am 30. Januar 2020 zum Thema «Wer kennt dich am besten? Du selbst, deine Familie und Freunde oder Facebook & Co.?» Die Gastreferenten Hans Kristoferitsch und Boris Treml aus Wien beschäftigten sich mit der Frage, was soziale Medien alles über die einzelnen (privaten) Nutzer wissen, die oft und gerne freizügig Informationen zu ihrer Person und ihrem Alltag auf Facebook, Instagram & Co. teilen. Die beiden Referenten erläuterten den 200 Gästen, wie sie damit umgehen können und wie sie sich vor diesem grossen Wissensdurst der sozialen Medien schützen können. In der anschliessenden Podiumsdiskussion zeigten zwei weitere Podiumsteilnehmer auf, dass umgekehrt die sozialen Medien auch bewusst dazu genutzt werden können, um in kurzer Zeit ein breites Publikum für ein bestimmtes Anliegen zu erreichen.

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 erwähnt werden. Im Berichtsjahr hat die DSS den Fokus erweitert und begonnen, auch für andere Bevölkerungsgruppen Programme zu entwickeln. So hatte die im Vorjahr durchgeführte Umfrage in der Bevölkerung Liechtensteins zum Thema Datenschutz diverse Gebiete mit Handlungsbedarf für die DSS aufgezeigt.

Im Berichtsjahr wurden deshalb zunächst speziell für Seniorinnen und Senioren Informationen zur Regelung des digitalen Nachlasses zusammengestellt, welche nicht nur als Newsletter und auf der Internetseite der DSS veröffentlicht wurden, sondern auch dem Seniorenbund zur Verfügung gestellt und im Rahmen einer Veranstaltung in Kooperation mit dem Haus Gutenberg der Öffentlichkeit präsentiert wurden. Diese Informationsvermittlung und auch die Veranstaltung stiessen auf reges Interesse und zeigten auf, dass in diesem Bereich noch vielerlei Wissenslücken bestehen und das Thema von den Betroffenen häufig unterschätzt wird.

Daneben bildeten auch 2020 wieder Schülerinnen und Schüler sowie Lernende weitere Schwerpunkt-Gruppen im Veranstaltungsangebot der DSS. Anlässlich einer firmeninternen Veranstaltung für Lernende eines liechtensteinischen Betriebs beschäftigte sich die DSS in ihrer Präsentation mit dem Titel «datenSCHUTZ!?» vor allem mit Themen der «Medienkompetenz», erklärte das Internet, zeichnete eine «Traceroute» von TikTok auf und ging auf Fragen des «Internet und soziale Netzwerke» ein. Ebenfalls thematisiert wurde Tracking im Internet, z.B. das WhatsApp-Tracking «online».

An einer schulinternen Veranstaltung in Triesen befasste sich der Vortrag der DSS mit dem Titel «Datenschutz, Internet und Smartphones – Ein Blick hinter die Kulissen» mit unterschiedlichsten Fragen zu Themen wie der Sammlung von Daten, Facebook, Betriebssystemen von Smartphones, Messenger-Diensten oder datenschutzfreundlichen Einstellungen bei beliebten Apps. Ein weiteres Thema war das Recht am eigenen Bild sowie die physiologische und psychologische Wirkung sozialer Medien.

Auch künftig sollen verschiedene Teile der Bevölkerung regelmässig und bedarfsgerecht mit Informationen der DSS bedient werden. Betroffene Personen oder Organisationen sind ebenfalls eingeladen, dazu Vorschläge bei der DSS einzubringen.

Ein grosser Erfolg war darüber hinaus eine neue Art der Veranstaltung, welche die DSS im Berichtsjahr erstmals organisiert hat. So wurde an der Privaten Universität im Fürstentum Liechtenstein jeweils ein Workshop zu den Themen «Videoüberwachung» und «Beschäftigtendatenschutz» durchgeführt. Nach einer theoretischen Einführung in die rechtlichen Voraussetzungen für Videoüberwachungen bzw. für die Verarbeitung von Beschäftigtendaten erarbeiteten und diskutierten die Teilnehmenden in Kleingruppen jeweils vier Beispielfälle aus der Praxis. Dadurch sollte die Kompetenz der Teilnehmenden praxisnah gestärkt werden, die Zulässigkeit von Videoüberwachungssystemen bzw. der Verarbeitung von Beschäftigtendaten aus Datenschutzsicht zu beurteilen. Die grosse Zahl der Teilnehmenden und deren positive Rückmeldungen waren Anlass, diese Workshops als Veranstaltungsreihe in Kooperation mit der Privaten Universität weiterzuführen und auch im Folgejahr wieder zwei Workshops zu aktuellen Themen anzubieten.

Das für den 27. Oktober 2020 geplante Vernetzungstreffen, mit dem sich die DSS alljährlich an die Datenschutzbeauftragten richtet, musste leider abgesagt werden. Nachdem ein Schwerpunkt dieser Veranstaltung – wie der Name sagt – auf der Vernetzung und dem persönlichen Kennenlernen und Austausch der Datenschutzbeauftragten liegt, verzichtete die DSS darauf, das Treffen ersatzweise als Online-Veranstaltung durchzuführen. Stattdessen wurden die hierfür geplanten Themen dem erwarteten Zielpublikum mittels Newsletter vermittelt. Sobald es die Umstände zulassen, soll das Vernetzungstreffen im Folgejahr nachgeholt werden.

1.2 Vorträge

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

1.2.1 Kooperation mit den Universitäten in Liechtenstein

Auch im Berichtsjahr sollte wieder schwerpunktmässig mit den beiden Universitäten in Liechtenstein zusammengearbeitet und gemeinsame Veranstaltungen angeboten werden. Bedauerlicherweise mussten dann aber die meisten Veranstaltungen abgesagt werden oder sie konnten erst gar nicht organisiert werden. Davon betroffen war auch die Planung eines Zertifikatsstudienganges im IT- und Datenschutzrecht, der von der Universität Liechtenstein gemeinsam mit der DSS geplant war und im Mai des Berichtsjahres hätte beginnen sollen. Ziel des Lehrgangs war es, eine umfassende Ausbildung in Liechtenstein anzubieten, welche über die in den vergangenen Jahren angebotenen Kurz-Lehrgänge für Datenschutzbeauftragte hinausgeht. Gespräche der DSS mit Datenschutzbeauftragten und Unternehmen zeigen deutlich, dass hierfür ein grosser Bedarf besteht. Die DSS erachtet es folglich als wichtige Aufgabe, gemeinsam mit Bildungseinrichtungen in Liechtenstein eine solche Ausbildung lokal anzubieten und den Interessenten eine auf ihre Bedürfnisse zugeschnittene Ausbildungsmöglichkeit zur Verfügung zu stellen.

Durchgeführt werden konnte am 5. März 2020 ein Themenabend an der Universität Liechtenstein zur Frage von «Datenschutzrecht und Dashcams». Der Zweck von Dashcams besteht darin, das Umfeld des Autos aufzuzeichnen, um die Aufnahmen bei Vorfällen (z.B. Unfällen, Sachbeschädigungen etc.) zu verwenden. Das Aufnehmen des öffentlichen Raumes ist dabei nicht unproblematisch. Ob die Aufnahmen über eingebaute Kameras oder am Armaturenbrett angebrachte Dashcams oder auf andere Art erfolgen, ist aus datenschutzrechtlicher Sicht irrelevant. Die rechtliche Beurteilung ist bei jedem Kameratyp dieselbe:

1. Aufnahmen, welche zum ausschliesslich persönlichen oder familiären Gebrauch bestimmt sind, sind von der DSGVO und dem DSG ausgenommen. Vorausgesetzt, die Aufnahmen werden nicht weitergegeben oder veröffentlicht. Der Zweck für den ausschliesslich persönlichen oder familiären Gebrauch muss plausibel sein und nachgewiesen werden.
2. Aufnahmen, welche zum Zwecke der Beweissicherung getätigt werden, implizieren eine Weitergabe der Daten an Behörden (Polizei) oder Versicherungsgesellschaften. Diese fallen daher unter den Anwendungsbereich der DSGVO und des DSG. Eine klassische Dashcam erfüllt regelmässig diese Voraussetzung.

Sind DSGVO und DSG anwendbar wie im Fall einer klassischen Dashcam, so folgt die rechtliche Prüfung den nachstehenden Schritten:

1. Das Aufnehmen des öffentlichen Raumes (Strasse, Parkplätze, Bürgersteige etc.) ist zulässig, wenn sie durch eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO gerechtfertigt werden kann. Bei privaten Personen ist hierfür Art. 6 Abs. 1 Bst. f DSGVO einschlägig. Die Beweissicherung bei Unfällen stellt ein berechtigtes Interesse im Sinne dieser Bestimmung dar.
2. Das anlasslose Aufzeichnen des Verkehrs und des öffentlichen Raumes kann hingegen nicht

von einem berechtigten Interesse gedeckt sein und ist somit nicht zulässig. Das berechtigte Interesse beschränkt sich in der Regel auf Vorfälle, die zur Geltendmachung von Rechtsansprüchen relevant sein können. Die datenschutzrechtliche Zulässigkeit beschränkt sich daher auf die Sekunden vor, während und kurz nach einem Vorfall (z.B. Unfall oder Einbruch in ein Fahrzeug). Im Sinne des technischen Datenschutzes ist dabei sicherzustellen, dass der Vorgang des Überspielens der Aufnahmen (Ringspeicher) automatisch und ausserhalb des Wirkungsbereichs des Verantwortlichen vorgenommen wird. Dadurch kann sichergestellt werden, dass die Aufnahmen nicht zweckentfremdet genutzt werden können. Weitere Möglichkeiten, die allenfalls zielführend sind, sind technische Massnahmen wie Verpixelung und keine Möglichkeit der manuellen Aktivierung der Dashcam.

3. Das grösste datenschutzrechtliche Hindernis für die Zulässigkeit einer Dashcam ist die Informationspflicht gemäss Art. 13 DSGVO, der jeder Verantwortliche unterliegt. Demnach sind betroffene Personen zum Zeitpunkt der Erhebung der Daten über gewisse Elemente zu informieren. Da ein Unfall jedoch nicht voraussehbar ist, ist es praktisch unmöglich, dieser Informationspflicht vor oder während des Aufzeichnens nachzukommen.

Aus diesen Gründen sieht die DSS Dashcams als praktisch unzulässig an.

Am 28. September 2020 fand in Zusammenarbeit mit der Universität Liechtenstein ausserdem eine Veranstaltung zum Thema «Geheimnisschutz – Schutzobjekt Information» statt, an der die DSS mit einem Vortrag zum Thema «Datenschutz im Home-Office – Erfahrungswerte während des «Lockdown»» vertreten war. Beleuchtet wurden darin insbesondere (Software-) Lösungen zur Kommunikation, die datenschutzkonforme Benutzung von solchen und die Bedeutung der Frage, was dabei zu beachten ist. Im Weiteren wurde auf Regelungen im Home-Office eingegangen, wie zum Beispiel Kernpräsenzzeiten, Umgang mit betrieblichen (IT-) Sachmitteln oder den Einsatz von Privatgeräten für berufliche Zwecke. Ebenfalls wurde auch auf Fragen aus der Sicht der Arbeitnehmenden eingegangen wie etwa auf die Frage, mit welchen Massnahmen der Arbeitgeber Mitarbeitende überwachen darf.

Am 1. Dezember 2020 fand an der Privaten Universität im Fürstentum Liechtenstein zum zweiten Mal in Folge eine eintägige Weiterbildungsveranstaltung zum Thema «Stolpersteine bei der Anwendung der DSGVO: was Unternehmen beachten sollten» statt. Der Vortrag der DSS im Rahmen der online durchgeführten Veranstaltung befasste sich mit dem aktuellen Thema «Datentransfer in Drittstaaten: Wie weiter nach dem EuGH Urteil Schrems II». Obwohl Liechtenstein nicht Mitgliedstaat der Europäischen Union ist, entfaltet das Urteil hierzulande ebenfalls unmittelbare Wirkung, da auch für liechtensteinische Verantwortliche und Auftragsverarbeiter der entsprechende Angemessenheitsbeschluss (EU-U.S. Privacy Shield) wegfiel und sie seitdem verpflichtet sind, eine alternative Rechtsgrundlage unter Kapitel V der DSGVO für Datentransfers in die USA zu suchen. Formell bestätigt wurde diese Tatsache mit dem EWR-Übernahmebeschluss zur Löschung des Durchführungsbeschlusses (EU) 2016/1250 aus Anhang XI des EWR-Abkommens, der am 11. Dezember 2020 unterzeichnet und am Folgetag in Kraft trat.

1.2.2 Weitere Vorträge

Neben den genannten grösseren Veranstaltungen nahmen Mitarbeitende der DSS auch an Veranstaltungen von Unternehmen für ihre Lernenden, an Kursen für Gastwirte sowie für Sachbearbeiterinnen und Sachbearbeiter, an einer Veranstaltung von Amnesty International sowie an mehreren Veranstaltungen an verschiedenen Schulen teil und präsentierten Beiträge zu unterschiedlichen Themen im Bereich Datenschutz. Dazu kam eine Veranstaltung des Privacy-Rings in Wien und zwei Veranstaltungen in Zürich. Diese Veranstaltungen in den Nachbarstaaten standen vor allem im Zeichen der Kooperation der DSS mit Datenschutzbehörden im nahen Ausland sowie dort ansässigen Datenschutzvereinigungen.

1.2.3 Besonderheit 2020: Teilnahme Ferienspass 2020

Nachdem im Frühjahr zahlreiche Veranstaltungen wegen der Corona-Massnahmen ausfallen mussten, darunter auch solche für Kinder und Jugendliche, entschied sich die DSS, am Projekt des Amtes für Soziale Dienste «ferienspass.li» teilzunehmen. Konkret bot die DSS im Rahmen dieses Ferienprogramms für Kinder zwei Nachmittagsveranstaltungen an mit dem Titel «Internet-Surfschein: Smarter Umgang mit Social Media, (Online-) Games und dem Internet». Angesprochen waren Kinder zwischen 8 und 10 sowie zwischen 11 und 13 Jahren. Auf dem Programm standen eine Einführung in die Welt des Internets und dessen Hintergründe sowie zahlreiche Fragen, die sich rund um das Internet und die sozialen Medien stellen. Beide Veranstaltungen waren schnell ausgebucht und stiessen auf grosses Interesse bei Eltern und Kindern.

1.3 Internetseite

Zwei wesentliche Elemente der Öffentlichkeitsarbeit sind der Internetauftritt sowie der circa zweimal monatlich versandte Newsletter der DSS. 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 wie bereits im Vorjahr 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 Datenschutz und Covid-19, zum Brexit oder zum Schrems II-Urteil, aber auch ausführliche Informationen zur Videoüberwachung (inkl. Drohnen, Wildtierkameras, Videoüberwachung im Nachbarschaftsbereich etc.), Checklisten zur Regelung des digitalen Nachlasses oder ein Judikaturspiegel mit einschlägiger Rechtsprechung der letzten Jahre. Speziell für Unternehmen hat die DSS ausserdem ihren Leitfaden zur Umsetzung datenschutzrechtlicher Pflichten überarbeitet sowie anwendungsorientierte Informationen zum Beschäftigtendatenschutz und zum Datenschutz im Home-Office zur Verfügung gestellt. Darüber hinaus wurden eine Vorlage für eine Vereinbarung über die gemeinsame Verantwortung nach Art. 26 DSGVO und eine Checkliste zur Abklärung der Erforderlichkeit einer Datenschutz-Folgenabschätzung entwickelt.

Die Internetseite der DSS mit ihrem breiten Informationsangebot erfreut sich dabei eines ungebrochenen Interesses. Einige Beiträge scheinen dabei von besonderer Relevanz für die Bevölkerung zu sein: So wurden mehr als die Hälfte aller Zugriffe im Berichtsjahr bei folgenden Beiträgen verzeichnet: «Berechtigtes Interesse» (21.9 %), «Muster und Checklisten» (18.1 %), «Für Unternehmen» (11.9 %), «Videoüberwachung/Drohnen» (9.2 %) sowie die unter der Rubrik «Veranstaltungen» aufgeführten Informationen (4.8 %).

1.4 Newsletter

Erfreulicherweise stiegen die Abonnentenzahlen auch im Berichtsjahr weiter deutlich an. Ende 2020 hatten 1'113 Personen den Newsletter der DSS abonniert. Dies entspricht einem Plus von 99 Personen gegenüber dem Vorjahr. 2020 hat die DSS insgesamt 23 Newsletter versandt.

Die Themenbereiche der im Berichtsjahr von der DSS versandten Newsletter umfassten nebst aktuellen Informationen in Zusammenhang mit Covid-19 (z.B. erlaubte Datenverarbeitung durch Behörden und Unternehmen, Regeln im Home-Office), zum Brexit oder zum Schrems II-Urteil etwa auch allgemeine Informationen zum Beschäftigtendatenschutz, zum überarbeiteten Leitfaden datenschutzrechtlicher Pflichten

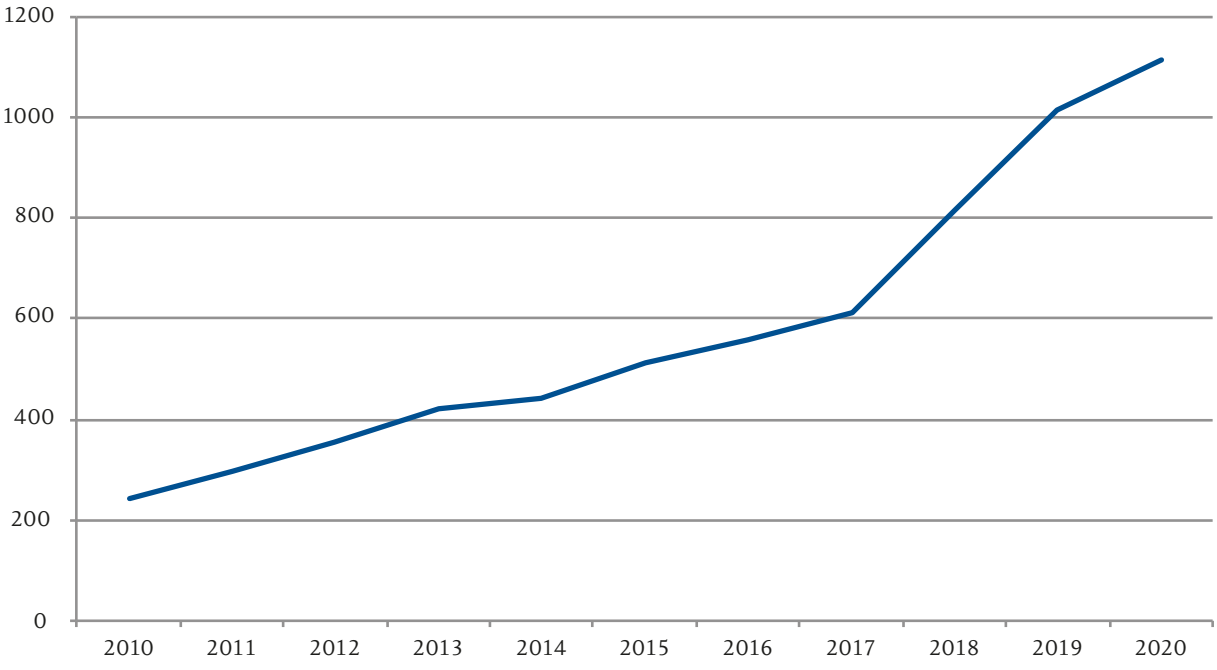


Abbildung 1: Entwicklung Newsletter Abonnenten

für Unternehmen, zur Regelung des digitalen Nachlasses, zum Datenschutz für Vermieter oder zur Veröffentlichung der Ergebnisse der von der DSS 2019 durchgeführten Umfrage. Bei der Wahl der Inhalte berücksichtigte die DSS soweit möglich die Bedürfnisse der Adressatinnen und Adressaten und reagierte auf verstärkte Anfragen zu bestimmten Themen. So erarbeitete die DSS auf Anregung von betrieblichen Datenschutzbeauftragten zum Beispiel auch eine Mustervereinbarung für eine gemeinsame Verantwortlichkeit gemäss Art. 26 DSGVO, eine Verfahrensbeschreibung für Datenschutzprüfungen oder eine Checkliste zur Beurteilung der Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung. Gehäufte Anfragen zu diversen Formen der Videoüberwachung (z.B. Wildtierkameras, Drohnen, Dashcams, Videoüberwachung im Nachbarschaftsbereich) gaben ebenfalls Anlass zum Versand von mehreren Newslettern und der Bereitstellung detaillierter Informationen dazu auf der Internetseite.

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 zu müssen.

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

1.5 Datenschutz in den Medien

Im Berichtsjahr war der Datenschutz wieder prominent in den liechtensteinischen Medien vertreten, allerdings waren auch hier die Schwerpunkte mehrheitlich von der Corona-Pandemie bestimmt. Themen der knapp 30 Berichte in den Printmedien waren neben zahlreichen Berichterstattungen zu den Corona-Apps auch der Datenschutztag 2020, der Tätigkeitsbericht der DSS, Datenschutz im Home-Office, Drohnen, die Blockchain, Datenschutz und Kontenregister oder das elektronische Gesundheitsregister.

Im Juni 2020 wurde die DSS von Radio L mit einer Interview-Anfrage im Kontext «Datenschutz in der Corona-Pandemie» kontaktiert. Schwerpunkt des Interviews waren vor allem verschiedene datenschutzrechtliche Untersuchungen rund um das Thema der Corona Warn-Apps. Durch Aufzeigen verschiedener Konzepte, mittels derer die Corona Warn-Apps in Europa umgesetzt wurden (z.B. zentraler oder dezentraler Ansatz), konnte dargelegt werden, dass eine datenschutzkonforme Umsetzung solcher Warn-Apps möglich ist. Die unterschiedlichen nationalen Gesetzgebungen und technischen Konzepte führen aber leider zu einer eingeschränkten grenzüberschreitenden Einsatzmöglichkeit der Apps. Innerhalb der Europäischen Union sind deshalb auf mehreren Ebenen Bestrebungen im Gange, die fehlende Interoperabilität solcher Apps noch herzustellen. In Liechtenstein beschloss die Regierung, unter anderem wegen des datenschutzfreundlichen Konzepts, die Schweizer Lösung (SwissCovid App) einzusetzen.

Die DSS analysierte im Auftrag der Regierung im Juni 2020 noch eine alternative Corona Warn-App, welche in einem zweiten Interview bei Radio L am 17. Juli 2020 Gegenstand des Gesprächs war.

Die vielfältige Berichterstattung in den Medien sowie deren positive Haltung gegenüber dem Datenschutz ist ein wertvoller Beitrag zur Umsetzung des kommunikativen Konzepts der DSS, da so die Information auch für Bürgerinnen und Bürger greifbar wird, die von Berufs wegen weniger Berührungspunkte mit Datenschutz haben.

«Insgesamt war wie bereits im Vorjahr eine deutliche Steigerung der Komplexität der Anfragen zu verzeichnen, welche im Berichtsjahr nochmals zunahm.»

2. Beratung in Bezug auf konkrete Anfragen

2.1 Allgemeines

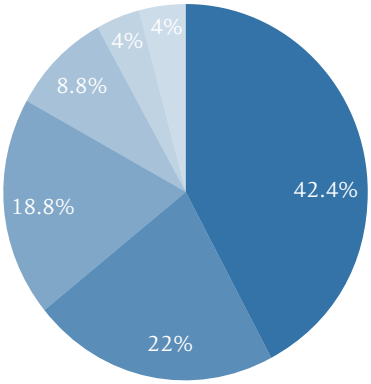
Im Berichtsjahr verzeichnete die DSS 1'544 Anfragen von öffentlichen und privaten Institutionen sowie Privatpersonen. Im Vergleich zu den im Vorjahr beantworteten 1'982 Anfragen bedeutet dies einen Rückgang von 438. Besonders merklich zeichnete sich der Rückgang in den Monaten März bis Mai ab, als vor allem Unternehmen vorrangig mit der Anpassung an die Covid-19-Pandemie sowie damit zusammenhängende Massnahmen beschäftigt waren und Datenschutzfragen etwas in den Hintergrund rückten.

Insgesamt war aber wie bereits im Vorjahr eine deutliche Steigerung der Komplexität der Anfragen zu verzeichnen, welche im Berichtsjahr nochmals zunahm. Dies war einerseits den vielen Fragen geschuldet, die mit der Covid-19-Pandemie verbunden waren und umfangreiche Evaluationen und Abklärungen erforderten, wie etwa die datenschutzrechtliche Zulässigkeit von Corona-Apps oder von Video- und Onlinekonferenzsoftware, die Verarbeitung und Weitergabe von Daten durch den Arbeitgeber zum Zwecke der Krankheitsprävention oder Datenschutz im Home-Office. Andererseits warf auch der technische Fortschritt zahlreiche neue und herausfordernde Fragen auf, ob und inwieweit bestimmte technische Systeme die Datenschutzanforderungen erfüllen. Dies betraf nicht nur die viel diskutierten Corona-Apps, sondern auch Forschungsprojekte im Gesundheitsbereich oder Fahrerassistenzsysteme in Kraftfahrzeugen. Auch die Prüfung des Einsatzes von Videoüberwachungsanlagen durch Privatpersonen, Unternehmen oder öffentliche Stellen erforderte Kenntnisse im rechtlichen wie auch technischen Bereich.

In Bezug auf die Herkunft der Fragesteller ist festzuhalten, dass diese dem Trend des letzten Jahres folgend zu einem grossen Teil aus der Privatwirtschaft stammten (42.4 %). Nicht ganz die Hälfte dieser Anfragen wiederum kam von kleinen und mittleren Unternehmen sowie Kleinstunternehmen. An zweiter und dritter Stelle folgten internationale Anfragen (22 %) sowie Anfragen der Landesverwaltung und Gemeinden (18.8 %). Privatpersonen machten 8.8 % der Fragesteller aus und zeigten damit erneut reges Interesse am Datenschutz. Die Anfragen von den Medien verblieben im Berichtsjahr auf dem Niveau des Vorjahres, konzentrierten sich allerdings mehrheitlich auf Themen mit Bezug zur Corona-Pandemie. In Bezug auf die Branchen stammten die meisten Anfragen im Berichtsjahr von Anwaltskanzleien und aus dem Finanzsektor.

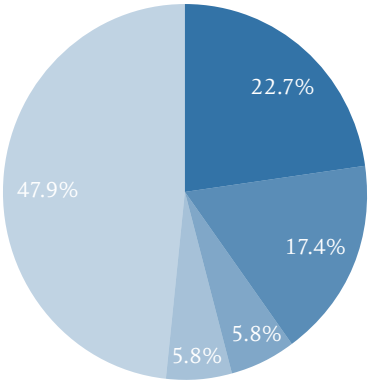
Beratungsanfragen konnten telefonisch, schriftlich – insbesondere mittels E-Mail – oder auch in einem persönlichen Gespräch bei der DSS eingebracht werden. Von den 1'544 Anfragen wurden im Berichtsjahr lediglich 214 telefonisch gestellt und beantwor-

Wer stellt die Fragen?



- Privatwirtschaft
- Internationales
- Behörden
- Privatpersonen
- Vereine
- Medien

Verteilung der Anfragen aus der Privatwirtschaft



- Anwaltskanzleien
- Banken, Vermögensverwaltung, und Treuhand
- Gesundheitswesen
- Versicherungen
- Andere

tet, während 2018 und 2019 noch 687 bzw. 413 Anrufer verzeichnet wurden. 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 im Berichtsjahr wieder die Frage, ob und in welchem Ausmass eine Datenschutz-Aufsichtsbehörde überhaupt beratend tätig sein sollte bzw. ob Aufsicht durch Beratung überhaupt im Sinne der DSGVO ist. Die DSS blieb auch im Berichtsjahr bei ihrer 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».

Die obige Fragestellung wurde im Berichtsjahr jedoch um eine zusätzliche Komponente ergänzt, welche die Frage betraf, inwieweit die DSS auch in einem Beschwerdeverfahren gemäss Art. 57 Abs. 1 Bst. f DSGVO oder einer Untersuchung gemäss Art. 57 Abs. 1 Bst. h DSGVO beratend tätig werden darf. So wurde die DSS in mehreren Verfahren von den Verantwortlichen ersucht, ihnen bei der Umsetzung der Vorgaben bzw. Anweisungen der DSS beratend zur Seite zu stehen. Die DSS hält jedoch 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 daher 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

Mit Inkrafttreten des DSG erfuhr die Videoüberwachung öffentlich zugänglicher Räume in Art. 5 eine neue gesetzliche Regelung. Wie die DSS in ihrem letzten Tätigkeitsbericht erläuterte, nahmen in Folge dessen die Anfragen zur Videoüberwachung stark zu. Dieser Trend hielt auch im Berichtsjahr 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.

So wurde die DSS im Berichtsjahr von mehreren Privatpersonen bezüglich Videoüberwachungen an Privatgrundstücken zu Wohnzwecken kontaktiert. Dabei steht oft die Zutrittskontrolle, die Durchsetzung des Hausrechts wie auch der Schutz vor Einbruch, Diebstahl und Vandalismus und der damit verbundenen Beweissicherung im Vordergrund. Daneben befasste sich die DSS auch mit der Zulässigkeit von Türspion-Kameras in solchen Kontexten.

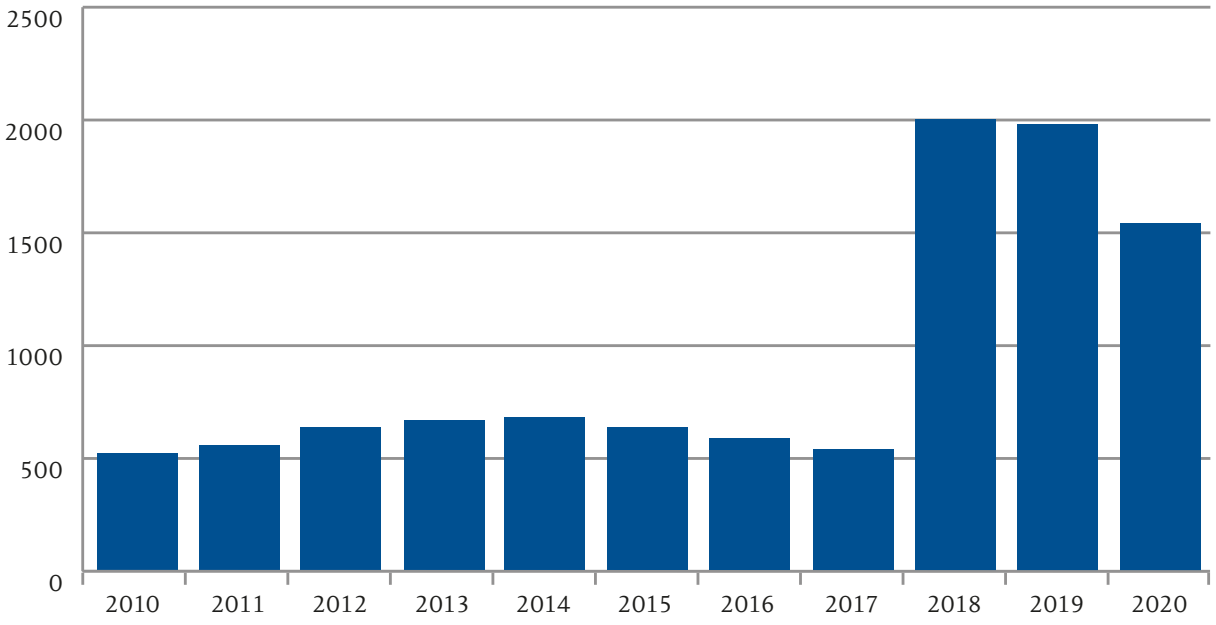


Abbildung 2: Anzahl der Anfragen von 2010 bis 2020

Zudem kamen im Berichtsjahr mehrere Unternehmen auf die DSS zu und konsultierten sie vorgängig der Umsetzung einer Videoüberwachungsanlage bezüglich deren datenschutzrechtlicher Machbarkeit. Die DSS nimmt diesbezüglich gerne ihre beratende Funktion wahr und nimmt sich jeweils die Zeit, die Situation vor Ort zu beurteilen und einzuschätzen.

Aber auch bei öffentlich-rechtlichen Stellen sind Videoüberwachungen aktueller denn je. Die DSS wurde im Berichtsjahr sowohl von einigen Gemeinden als auch von der Liechtensteinischen Landesverwaltung bezüglich bestehender wie auch gewünschter Videoüberwachungen kontaktiert. Hierbei ist insbesondere der Fall einer schon seit längerem bestehenden Videoüberwachungsanlage an einer öffentlich zugänglichen Freizeitanlage zu erwähnen. Im Rahmen der kooperativen Gespräche mit dem Verantwortlichen hat die DSS darauf hingewirkt, dass die Videoüberwachung auf das absolut erforderliche Mass beschränkt wurde, denn das Freizeitverhalten der Bürgerinnen und Bürger ist als besonders schützenswert zu qualifizieren und kann und darf daher nur aus besonders triftigen Gründen überwacht werden. Diese liegen bei allgemein zugänglichen Freizeiteinrichtungen regelmässig nicht vor.

In Bezug auf die mit Art. 5 Abs. 7 DSG sowie Art. 5 DSV eingeführte Meldepflicht von Videoüberwachungen sind im Berichtsjahr 13 Drohnenflüge, 38 Videoüberwachungsanlagen und eine Wildtierkamera bei der DSS gemeldet worden.

2.3 Verbindliche interne Datenschutzvorschriften

Seit 2019 betreut und berät die DSS als federführende Behörde ein weltweit tätiges, liechtensteinisches Unternehmen in der Ausarbeitung von verbindlichen internen Datenschutzvorschriften («Binding Corporate Rules»; BCR) für sämtliche seiner Unternehmenseinheiten. Die Arbeiten an diesen internen Datenschutzvorschriften erzielten im Berichtsjahr sehr gute Fortschritte und sollten im Folgejahr abgeschlossen werden können.

2.4 Datenschutzrechtliche Überprüfung von Covid-19 Tracing-Apps

Die DSS wurde Anfang Mai von der Regierung ersucht, eine Covid-19 Tracing-App einer datenschutzrechtlichen Beurteilung zu unterziehen. Vor der eigentlichen Überprüfung der App wurden die verschiedenen technischen Konzepte, die bereits im Ausland als Basis für die Umsetzung der länderspezifischen Corona Tracing Apps dienten, anhand öffentlich verfügbarer Dokumente sowie teilweise bereits durchgeführter Datenschutz-Folgenabschätzungen gemäss Art. 35 DSGVO analysiert. Da die konkrete App im Hintergrund auf dem sogenannten Distributed privacy-preserving contact tracing (DP3T) Protokoll aufbaut, waren die Recherchen im Vorfeld sehr hilfreich für das bessere Verstehen des Datenflusses im Hintergrund als auch für die folgende Überprüfung der App. Der abschliessende Bericht der DSS wurde am 22. Juli an die Regierung übermittelt. Dabei erachtete die DSS den Einsatz der App als datenschutzrechtlich zulässig und begründete dies folgendermassen:

«Durch angemessene technische und organisatorische Massnahmen ist die Datenverarbeitung durch die App so ausgestaltet, dass diese zweckmässig und auf das erforderliche Mass reduziert ist. Aufgrund dieser Eingrenzungen und der umgesetzten Massnahmen ist die Datenverarbeitung durch die App auch gegenüber den Risken einer Verletzung der Rechte Betroffener als verhältnismässig einzustufen.» Trotz einer datenschutzkonformen Ausgestaltung der App erachtet die DSS Covid-19 Tracing-Apps im Allgemeinen nicht als Allheilmittel, sondern als sinnvolle Ergänzung zu weiteren Massnahmen im Kampf gegen die Pandemie.

Im Gegensatz zum dezentralen Ansatz wurde gerade zu Beginn der Entwicklungsphase der Corona Tracing Apps ein zentraler Ansatz (Pan-European Privay-Preserving Proximity Tracing – PEPP-PT) von einigen Ländern in der EU, als auch der Schweiz verfolgt. Aus Datenschutzperspektive wurde die Entwicklung des Standards bzw. einer Europäischen Plattform, bei der persönliche Daten – wenn auch pseudonymisiert – auf einer zentralen Instanz gespeichert werden, kritisch beobachtet. Nachdem sich immer mehr Forscherinnen und Forscher gegen die Umsetzung eines zentralen Ansatzes ausgesprochen haben, kehrten einige Länder, darunter Deutschland, Italien als auch die Schweiz, von der zentralen Methode ab und wandten sich dem datenschutzfreundlicheren DP3T Verfahren zu. Andere Länder wie z.B. Frankreich oder Ungarn setzten weiterhin auf einen zentralen Ansatz.

Aufgrund dieser unterschiedlichen technischen Konzepte als auch rechtlichen Grundlagen, konnte das Problem der Interoperabilität erst gegen Ende 2020 entschärft werden, als die EU am 19. Oktober 2020 die Inbetriebnahme des EU-Datenabgleichdienstes verkündete. Somit war erstmals, wenn zu Beginn auch eingeschränkt, der grenzüberschreitende Austausch von Daten möglich, so dass Infektionsketten auch international nachverfolgt und bestenfalls unterbrochen werden konnten. Die Einbindung der Schweizer SwissCovid App ist aufgrund fehlender Rechtsgrundlagen bis heute nicht vorgesehen. Da Liechtenstein ebenfalls die Nutzung der SwissCovid App nahelegt,

ist auch hier der Datenaustausch mit EU-Mitgliedstaaten nicht möglich.

2.5 Technischer Datenschutz

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

Ist es für die Verarbeitung von Personendaten nach dem sogenannten Schrems II-Urteil des EuGH vom 16. Juli 2020 nach wie vor zulässig, amerikanische Software zu verwenden, oder muss komplett darauf verzichtet werden?

Es kommt in Bezug auf das erwähnte Urteil des EuGH bei der Prüfung und Beurteilung von (technischen) Lösungen vor allem darauf an, ob es bei der Datenverarbeitung im EWR gleichzeitig auch zu einer Übermittlung von personenbezogenen Daten in den Drittstaat USA kommt. Es gibt durchaus IT-Produkte, die zwar ihren Ursprung in den USA haben, in Europa aber so eingesetzt werden können, dass es bei der Anwendung zu keinem Datentransfer in die USA kommt. IT-Lösungen und Software im weitesten Sinn verändern sich durch fortlaufende Updates ständig. Das eingesetzte Lizenzmodell, die konkrete Version einer Software und insbesondere die Konfiguration sind zu berücksichtigen, denn häufig hängen davon allfällige Datenübermittlungen in die USA ab. Die Frage, ob der Einsatz einer Software datenschutzkonform ist, kann deshalb nicht pauschal beantwortet werden. So bedarf es immer einer Einzelfallprüfung. Lediglich im Falle einer tatsächlichen Datenübermittlung in die USA liegt es in der Verantwortung des «Datenexporteurs» sicherzustellen, dass nebst geeigneten Garantien gemäss Art. 46 ff. DSGVO eine DSGVO-konforme Datenübermittlung sichergestellt werden kann. Der EuGH legt in seinem Urteil dabei nicht fest, um welche zusätzlichen Garantien oder Massnahmen es sich dabei handeln könnte.

Ist die der Einsatz von Google Analytics oder Mailchimp nach dem Schrems II-Urteil des EuGH vom 16. Juli 2020 noch zulässig?

Bei der Einbindung von Google Analytics werden faktisch immer personenbezogene Daten verarbeitet bzw. an Google in die USA übermittelt. Selbst die sogenannte IP-Maskierung bietet aufgrund zusätzlich zur Anwendung kommender Techniken wie dem Setzen bzw. Auslesen von Cookies, der Übertragung der URL der besuchten Internetseite, der Verarbeitung der eindeutigen Kennung (ID) für Werbezwecke etc. keinen ausreichenden Schutz für betroffene Personen im Kontext des Schrems II-Urteils. Daher ist aus Sicht der DSS ein DSGVO-konformer Einsatz von Google Analytics derzeit nicht möglich.

Beim U.S.-Anbieter Mailchimp ist eine DSGVO-konforme Ausgestaltung derzeit ebenso wenig umsetzbar, da personenbezogene Daten ausschliesslich in die USA übertragen und dort gespeichert werden. Zudem führt Mailchimp auf seiner Internetseite im Annex D des Data Processing Addendum aus, dass einem Rechtsbehelf unter gewissen Voraussetzungen nicht nachgekommen werden kann. Des Weiteren umfasst die Liste der Unterauftragsverarbeiter fast ausschliesslich U.S.-Unternehmen, die wiederum den im Schrems II-Urteil erwähnten Zugriffsmöglichkeiten durch die U.S.-Regierung unterliegen.

Für welche Datenverarbeitungen ist eine Datenschutz-Folgenabschätzung durchzuführen?

Eine Datenschutz-Folgenabschätzung (DSFA) ist für so manche, aber nicht für alle Verarbeitungsvorgänge von personenbezogenen Daten vorgeschrieben, bei denen die Möglichkeit eines Risikos für die Rechte und Freiheiten natürlicher Personen besteht. Gemäss Art. 35 DSGVO ist die Durchführung einer DSFA immer dann obligatorisch, wenn die Verarbeitung «voraussichtlich ein hohes Risiko» für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Dies betrifft sowohl geplante als auch bereits laufende Verarbeitungsvorgänge. Die DSS hat zur Orientierung eine Checkliste im Excel-Format erarbeitet, welche sich in sechs Abschnitte gliedert. Jeder Abschnitt umfasst einige Hauptfragen, mit deren Beantwortung in weiterer Folge festgestellt wird, ob die Notwendigkeit der Durchführung einer DSFA für eine bestimmte Verarbeitungstätigkeit besteht. Alternativ zu den Hauptfragen können ebenso mehrere erläuternde Unterfragen beantwortet werden. Die Checkliste ist auf der Internetseite der DSS abrufbar.[1]

Welche technischen und organisatorischen Massnahmen sind im Home-Office in Bezug auf den Datenschutz umzusetzen?

Diese Frage lässt sich nicht pauschal beantworten. Grundsätzlich gilt auch im Home-Office der risikobasierte Ansatz, d.h. je sensibler und damit schützenswerter personenbezogene Daten sind, desto stärker sind sie zu schützen. Als besonders wichtig erachtet die DSS eine vom Unternehmen kommunizierte Regelung für mobile Geräte, die Klarheit für die Mitarbeitenden im Umgang mit personenbezogenen Daten schafft. Insbesondere sollte der Arbeitgeber eine ent-

[1] https://www.datenschutzstelle.li/download_file/view/542.

sprechend geschützte IT-Infrastruktur zur Verfügung stellen, sodass die Vertraulichkeit, Verfügbarkeit und Integrität der Daten auch bei der Arbeit von zu Hause gewährleistet werden kann. Eine Checkliste für Benutzungsreglemente betreffend mobile Geräte ist auf der Internetseite der DSS abrufbar.[2] Neben den technischen Massnahmen sind im Home-Office aber ebenso organisatorische Massnahmen zu ergreifen, die sich nach den konkreten Verarbeitungstätigkeiten richten. Auch zu dieser Frage finden sich detaillierte Informationen auf der Internetseite der DSS.[3]

[2] https://www.datenschutzstelle.li/application/files/9616/0033/7138/pdf-llv-dss-checkliste_mobile_geraete.pdf
[3] https://www.datenschutzstelle.li/datenschutz/themen-z/datenschutz-am-arbeitsplatz

«Aufgrund der laufenden Digitalisierungs-Bestrebungen ist davon auszugehen, dass das ZPR künftig einen noch höheren Stellenwert erhalten wird, da es die zentrale Drehscheibe für einen wichtigen Teil der hierfür benötigten Daten darstellt.»

3. Stellungnahmen zu Vorlagen und Erlassen

3.1 Stellungnahme zum Gesetz über das Zentrale Personenregister (ZPRG)

Im Vernehmlassungsbericht vom Oktober 2020 wird ausgeführt, dass das Zentrale Personenregister (ZPR) seit langem und bis heute für die öffentlichen Stellen ein besonders wichtiges Arbeitsinstrument ist. Aufgrund der laufenden Digitalisierungs-Bestrebungen ist davon auszugehen, dass das ZPR künftig einen noch höheren Stellenwert erhalten wird, da es die zentrale Drehscheibe für einen wichtigen Teil der hierfür benötigten Daten darstellt. Die Regierung betont, dass das ZPR für effiziente, sichere und qualitativ hochstehende elektronische Dienstleistungen unerlässlich ist und sowohl den öffentlichen Stellen als auch deren Kunden vielfältige Möglichkeiten bietet. Die DSS unterstützte die Regierung bei der Ausarbeitung des Gesetzesentwurfes und sprach sich dabei dafür aus, dass das ZPR künftig aus datenschutzrechtlicher Sicht in gemeinsamer Verantwortung der öffentlichen Stellen eingerichtet und betrieben wird. Ebenso war es aus Sicht der DSS wesentlich, im Gesetz und den Erläuterungen explizit und deutlich hervorzuheben, dass der Zugriff auf diese Daten bzw. deren Verarbeitung durch die öffentlichen Stellen nur dann zulässig ist, wenn dies für die Erfüllung der ihnen gesetzlich übertragenen Aufgaben erforderlich ist. Dieser Grundsatz der Erforderlichkeit kommt im Gesetz nun prominent zum Ausdruck, was von der DSS ausdrücklich begrüsst wird. Zweifel blieben aus Sicht der DSS allerdings im Hinblick auf die Datenrichtigkeit bestehen, weshalb diese Thematik auch den Schwerpunkt ihrer Stellungnahme ausmachte.

Insgesamt werden im Vernehmlassungsbericht verschiedenste Begriffe und Bezeichnungen für die nähere Qualifizierung von Daten verwendet, so etwa «Authentizität von Daten», «authentische Originaldaten», «Echtheit und Richtigkeit der Daten», «authentische Datenquelle» oder «Datenqualität». Es stellte sich folglich die Frage, was genau mit diesen unterschiedlichen Begriffen ausgedrückt werden soll. Letztlich scheinen die Begriffe wohl auf den datenschutzrechtlich relevanten Begriff der «Richtigkeit der Daten» hinauszulaufen. Gemäss Art. 5 Abs. 1 Bst. d DSGVO müssen Daten «sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Massnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden («Richtigkeit»)». Wiederholt wird diese Verpflichtung auch in Art. 47 DSG.

Aufgrund der unterschiedlichen Terminologie im Vernehmlassungsbericht regte die DSS in ihrer Stellungnahme an, im gegenständlichen Gesetzesentwurf nur einen einzigen, einheitlichen Begriff für die nähere Qualifizierung von Daten zu verwenden und diesen in den Erläuterungen auch unmissverständlich im Sinne der Datenschutzgesetzgebung zu definieren. Es sollte so klargestellt sein, dass das ZPR im Sinne des Art. 5 Abs. 1 Bst. d DSGVO «richtige» Daten beinhaltet. Im Zusammenhang mit Digitalisierung und digitaler Transformation sind qualitativ fehlerfreie Personenstammdaten das Fundament jeden digitalen Vorhabens, weshalb die ZPR-Stammdaten zu 100 % richtig erfasst werden bzw. sein müssen.

Zudem sollte auch der weiteren Verpflichtung des Art. 5 Abs. 1 Bst. d DSGVO, nämlich der Anwendung von angemessenen Massnahmen zur unverzüglichen Löschung und Berichtigung von personenbezogenen Daten, mehr Raum und Bedeutung im revidierten ZPR-Gesetz eingeräumt werden. Aktuell vermitteln der Gesetzestext und die Erläuterungen den Eindruck, dass das ZPR ausschliesslich aus «richtigen» Daten besteht. Für den Fall von stets möglichen Unrichtigkeiten oder Mehrfachnennungen etc. empfiehlt die DSS deshalb, das Löschrecht nicht vollständig auszuschliessen. Es scheint darüber hinaus schwierig, einen kategorischen Ausschluss gegenüber den klaren Vorgaben des Art. 17 DSGVO bzw. Art. 35 DSG zu rechtfertigen.

Bei der Zusammensetzung der ZPR-Kommission stellte sich für die DSS die Frage, ob unter den Fachverantwortlichen nicht auch eine Person mit Rechtskenntnissen einschliesslich Datenschutz sein sollte. Das ZPR ist ein zentrales Instrument mit einer sehr weitreichenden Erfassung von personenbezogenen Daten. Aus diesem Grund sollte dem Datenschutz auch im «Betriebsalltag» eine aktive Rolle zukommen und eine Person mit dem nötigen Fachwissen an den Entscheidungen der ZPR-Kommission beteiligt sein. Dadurch wäre auch ein präventiver Datenschutz gewährleistet, während in der aktuellen Fassung des Gesetzes der Datenschutz erst nachträglich zum Tragen kommt, wenn bei festgestellten bzw. vermuteten Fehlern der DSS ein Zugriff auf die Protokolle erlaubt wird. Die DSS regte in ihrer Stellungnahme daher an, eine Juristin bzw. einen Juristen als Mitglied der ZPR-Kommission gesetzlich vorzusehen. Idealerweise sollte diese Person auch über Kenntnisse im Datenschutz verfügen.

3.2 Stellungnahme zur «Interoperabilität» europäischer Informationssysteme

Im Rahmen einer informellen Vernehmlassung wurde die DSS ersucht, sich zur Umsetzung der sogenannten «Interoperabilität» zu äussern. Dabei handelt es sich um zwei europäische Verordnungen (IOP-Verordnungen), die im Rahmen der Weiterentwicklung des Schengen-Besitzstandes zur Anwendung kommen und in nationales Gesetz übernommen werden sollen. Bereits heute werden von Grenzkontroll-, Migrations- und Strafverfolgungsbehörden unterschiedliche, europaweit implementierte Informationssysteme (Datenbanken) genutzt. Diese Systeme sind jedoch technisch nicht miteinander verbunden, was mit Blick auf die Gewährleistung der Sicherheit in Europa ein Manko darstellt. Diesem unbefriedigenden Umstand wird nun mit der Umsetzung einer Interoperabilität der verschiedenen Systeme Rechnung getragen. Dazu werden vier Interoperabilitätskomponenten eingeführt: 1. Über ein Europäisches Suchportal (ESP) soll eine Personen-Suche parallel in mehreren EU-Informationssystemen möglich sein; 2. Für einen gleichzeitigen Abgleich biometrischer Daten mit diesen Informationssystemen wird ein gemeinsamer Dienst (sBMS) eingeführt; 3. Mit einer (biometrischen) Abfrage des gemeinsamen Speichers für Identitätsdaten (CIR) kann Auskunft darüber erhalten werden, ob ein Drittstaatsangehöriger in mehreren der europäischen Datenbanken unter verschiedenen Identitäten registriert ist; und 4. Über einen Detektor für Mehrfachidentitäten (MID) sollen Mehrfachidentitäten aufgedeckt werden, die mit ein und demselben Satz an biometrischen Daten verknüpft sind.

Mit Hilfe der auf diese Weise geschaffenen Interoperabilität der verschiedenen Informationssysteme können beispielsweise Identitätsdaten, Daten zu Reisedokumenten und biometrische Daten (Fingerabdrücke und Gesichtsbilder) automatisiert abgeglichen und kriminelle Personen, welche falsche Identitäten benutzen, identifiziert werden. Ohne die Interoperabilität müsste jedes System jeweils einzeln abgefragt werden. Zentral ist dabei jedoch auch, dass die genau definierten Zugriffsberechtigungen der einzelnen Behörden auf die Systeme unverändert bleiben.[4]

Da in Zusammenhang mit den relevanten Informationssystemen und der geplanten Interoperabilität dieser Systeme umfangreiche und äusserst sensible (biometrische) personenbezogene Daten verarbeitet werden, hat die DSS die Gesetzesanpassung im Entwurf näher geprüft und detailliert Rückmeldung dazu gegeben. Neben einigen Kommentaren, Rückfragen und Anregungen hob die DSS insbesondere folgende Punkte hervor:

- Datenverarbeitungen im Rahmen der oben beschriebenen Interoperabilitätskomponenten bedürfen gemäss Art. 35 Abs. 1 und 3 Bst. b DSGVO und Art. 66 DSG einer Datenschutz-Folgenabschätzung (DSFA). Eine DSFA kann entweder schon im Rahmen des Gesetzgebungsverfahrens durchgeführt werden (Art. 35 Abs. 10 DSGVO), oder sie muss durch jede zuständige Behörde vor erstmaliger Durchführung vorgenommen werden.
- Die IOP-Verordnungen sehen vor, dass es eine Möglichkeit geben muss, jeden Missbrauch oder Verarbeitungen bzw. Austausch von Daten, die diesen Verordnungen zuwiderlaufen, zu ahnden. Damit zusammenhängende Sanktionen müssen wirksam, verhältnismässig und abschreckend sein. Da in der Vernehmlassungsvorlage kein Hinweis auf eine diesbezügliche nationale Umsetzung zu finden war, regte die DSS die Einführung eines Sanktionssystems analog demjenigen der DSGVO an. Konkret schlug die DSS eine entsprechende Anpassung von Art. 40 Abs. 7 DSG vor. Diesem Vorschlag wurde jedoch nicht gefolgt. Laut Bericht und Antrag der Regierung an den Landtag (BuA 66/2020) werden wirksame, verhältnismässige und abschreckende Sanktionen weiterhin durch den bestehenden Art. 86a AuG gewährleistet. Dies stellt aus datenschutzrechtlicher Sicht jedoch eine ungenügende Umsetzung der IOP-Verordnungen dar, weil Art. 86a AuG lediglich eine Sanktionsmöglichkeit bei Zuwiderhandlungen gegen nationales Recht vorsieht. Da nun aber nicht alle Bestimmungen der europäischen IOP-Verordnungen sinngemäss ins liechtensteinische Recht übernommen wurden, sondern einige auch direkt anwendbar sind, können mittels Art. 86a AuG wohl nicht alle missbräuchlichen Datenverarbeitungen nach den IOP-Verordnungen sanktioniert werden.
- Wenn gewisse Voraussetzungen erfüllt sind, zum Beispiel wenn sich eine Person nicht ausweisen kann, dann darf die Landespolizei zur Identifikation der Person mit ihren Fingerabdrücken neu einen Abgleich des CIR vornehmen. In Liechtenstein ist diese Möglichkeit jedoch ausschliesslich zur Identifikation von Drittstaatsangehörigen und unbekannten Personen im Fall eines Unfalls, einer Naturkatastrophe oder eines Terroranschlages vorgesehen (Art. 76c Abs. 1 AuG). Wie kann jedoch sichergestellt werden, dass ausschliess-

[4] Ausführlichere Informationen zur Interoperabilität sind im entsprechenden BuA 66/2020 zu finden.

lich biometrische Daten Drittstaatsangehöriger mit dem CIR abgeglichen werden, wenn sich die betroffenen Personen nicht ausweisen können? Dies öffnet einer Diskriminierung aufgrund der Sprache, Rasse und Hautfarbe, ethnischen oder sozialen Herkunft Tür und Tor. Diese Gefahr hat offensichtlich auch der EU-Gesetzgeber erkannt und das Diskriminierungsverbot nochmals explizit in Art. 5 der IOP-Verordnungen statuiert. In ihrer Stellungnahme hat auch die DSS auf diese möglichen Grundrechtsverletzungen in der praktischen Umsetzung von Abgleichen mit dem CIR hingewiesen. Da im Berichtsjahr nicht geklärt werden konnte, wie Abgleiche des CIR vollständig gesetzeskonform durchgeführt werden können, wird die DSS die Implementierung und Umsetzung entsprechender Massnahmen insbesondere durch die Landespolizei weiter beobachten und bei Bedarf auch beratend zur Seite stehen.

Aufgrund des Umfangs und der Sensibilität der Datenverarbeitungen in Zusammenhang mit der Interoperabilität europäischer Informationssysteme wie auch aufgrund der Notwendigkeit einer mindestens alle vier Jahre durchzuführenden datenschutzrechtlichen Aufsicht (Art. 51 Abs. 3 IOP-Verordnungen), wird die DSS diese Thematik nicht aus den Augen verlieren und gegebenenfalls Kontrollen durchführen.

3.3 Weitere Stellungnahmen

Darüber hinaus verfasste die DSS im Berichtsjahr weitere inhaltliche Stellungnahmen zu den folgenden acht Vernehmlassungsberichten der Regierung:

- Abänderung der Zivilprozessordnung (ZPO) und des Ausserstreitgesetzes (AussStrG) im Zuge der Ratifizierung des Übereinkommens des Europarats vom 11. Mai 2011 zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (Istanbul-Konvention);
- Abänderung des Sozialhilfegesetzes (Fürsorgerische Unterbringung und Heimaufenthalt);
- Abänderung des Personen- und Gesellschaftsrechts (PGR) sowie des Bankengesetzes (BankG) zur Umsetzung der Richtlinie (EU) 2017/828;
- Abänderung des Mediengesetzes (MedienG) und des Tabakpräventionsgesetzes (TPG) zur Umsetzung der Richtlinie (EU) 2018/1808;
- Abänderung des Strafgesetzbuches (StGB), der Strafprozessordnung (StPO), des Rechtshilfegesetzes (RHG) und weiterer Gesetze;
- Abänderung des AIA-Gesetzes, des FATCA-Gesetzes, des AStA-Gesetzes, des CbC-Gesetzes sowie des Steuergesetzes (SteG);
- Abänderung des Gesetzes über bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (UCITSG) und des Gesetzes über die Verwalter alternativer Investmentfonds (AIFMG) sowie des Gesetzes über die Finanzmarktaufsicht (FMAG); sowie
- Abänderung des Gesetzes über die amtliche Schätzung von Grundstücken und Gebäuden (SchätzG).

Die Prüfung von 12 weiteren Vorlagen ergab keine datenschutzrechtlichen Bedenken, weswegen auf eine Stellungnahme verzichtet wurde.

«Die Entscheidung, das Team im Vorjahr mit einem zweiten Techniker zu verstärken, erwies sich insbesondere im Berichtsjahr als richtig, denn die technischen Fragestellungen nahmen 2020 deutlich zu.»

4. Interne Organisation

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

Entsprechend Art. 14 Abs. 7 DSG legte die DSS im Berichtsjahr dem Ministerium für Justiz, Äusseres und Kultur ein Organisationsreglement vor, welches die Regierung zur Kenntnis nahm.

4.1 Personal allgemein

Die DSS konnte die an sie gestellten Anforderungen im Berichtsjahr mit dem bestehenden Personal von 700 Stellenprozenten sehr gut erfüllen. Die Entscheidung, das Team im Vorjahr mit einem zweiten Techniker zu verstärken, erwies sich insbesondere im Berichtsjahr als richtig, denn die technischen Fragestellungen nahmen 2020 deutlich zu. Zudem stellte sich heraus, dass selbst bei rechtlichen Fragen zunehmend technische Elemente involviert sind, die es bei der Beantwortung zu berücksichtigen gilt. Art. 32 DSGVO fordert etwa, dass der Verantwortliche «technische und organisatorische Massnahmen [trifft], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten». Für Juristen ist die Beurteilung dieses angemessenen Schutzes bzw. der dafür erforderlichen technischen und organisatorischen Massnahmen zunehmend schwierig, wodurch die beiden Techniker der DSS im Berichtsjahr wesentlich öfter in die Beantwortung von Anfragen und natürlich auch in Untersuchungen im Falle von Beschwerden einbezogen werden mussten.

Daneben forderte die Zunahme der Komplexität der Anfragen und Beschwerden einiges an Mehrleistung von den Mitarbeitenden der DSS. Zudem mussten im Falle von nicht-deutschsprachigen Beschwerdeführern im Berichtsjahr mehrere Verfahren in englischer Sprache geführt werden. Auch die Teilnahme an den Sitzungen des Europäischen Datenschutz-Ausschusses und seiner Arbeitsgruppen erforderte im Berichtsjahr sehr gute Englischkenntnisse der Mitarbeitenden der DSS, da aufgrund der mittels Videokonferenzen digital durchgeführten Sitzungen keine Dolmetschdienste zur Verfügung standen und die Sitzungen ausschliesslich in englischer Sprache durchgeführt wurden.

Schliesslich konnte die DSS im Berichtsjahr erstmals einen Praktikanten beschäftigen. Der Praktikant mit rechtswissenschaftlicher Ausbildung verstärkte das Team der DSS zwischen September und Ende Dezember mit einem Pensum von 80 Stellenprozenten.

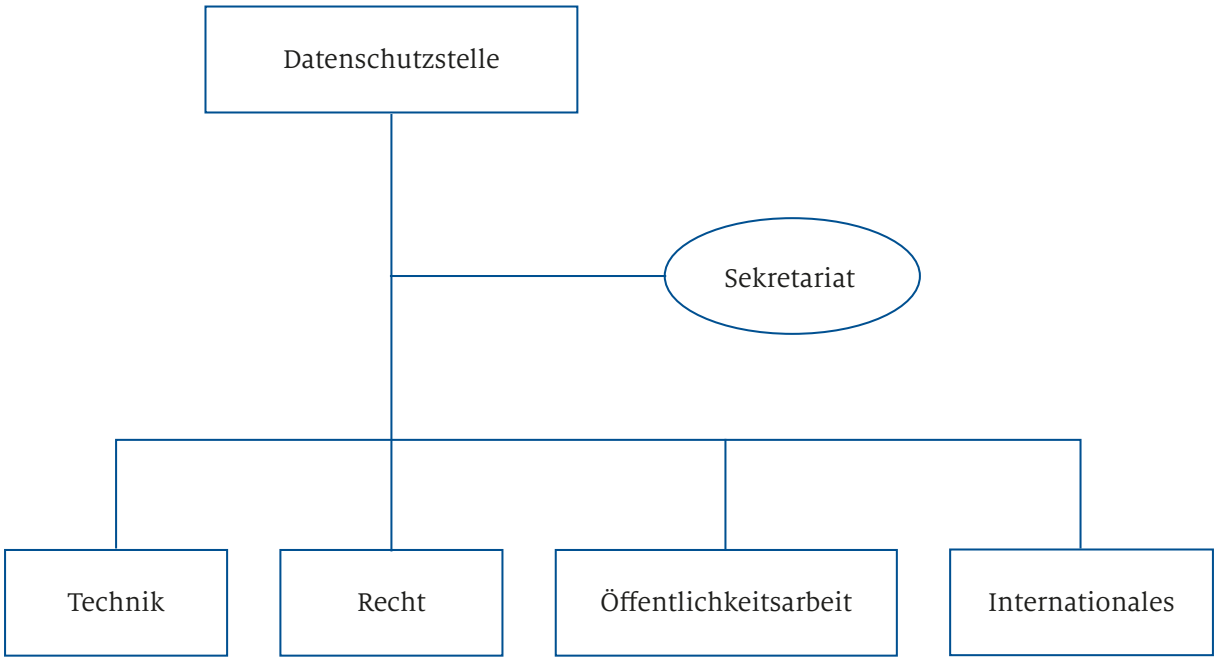


Abbildung 3: Organigramm Datenschutzstelle

Dank seines akademischen Hintergrundes konnte er vor allem bei Recherchetätigkeiten wertvolle Dienste leisten und zusätzlich das Team in allen Bereichen unterstützen.

4.2 Personal Schengen-Evaluation

Die gesetzlichen Grundlagen diverser EU-Informationssysteme sehen vor, dass diese alle vier Jahre einer datenschutzrechtlichen Kontrolle unterzogen werden müssen. Bis 2019 konnten diese datenschutzrechtlichen Kontrollen auf Grund begrenzter personeller Ressourcen der DSS nicht oder nur in sehr eingeschränktem Rahmen durchgeführt werden. Der 2019 gestellte Antrag auf Erhöhung des Personals der DSS war daher unter anderem mit der Notwendigkeit der Schengen-Kontrollen begründet. Die vom Landtag 2019 bewilligte Stelle erlaubte es der DSS, ihren Verpflichtungen im Rahmen der Teilnahme Liechtensteins am Schengen-Raum im Berichtsjahr vollumfänglich nachzukommen. So hatte die DSS bereits im Jahr 2019 zwei Kontrollen initiiert. Bei der datenschutzrechtlichen Überprüfung des Schengener Informationssystems wurde der Umfang und Gegenstand auf jene Bereiche eingeschränkt, welche die grössten Risiken für die betroffenen Personen bergen oder welche bei vergangenen Datenschutzüberprüfungen durch die DSS noch nicht geprüft wurden. Da das Visa-Informationssystem durch die DSS ebenfalls noch nie überprüft worden war, wurde auch hierfür eine umfassende Kontrolle lanciert. In beiden Fällen wurde im Berichtsjahr jeweils eine vor-Ort-Kontrolle bei den zuständigen Behörden durchgeführt und die Überprüfung danach erfolgreich abgeschlossen. Die im Rahmen der Kontrollen getroffenen Feststellungen werden im Nachgang von den zuständigen Behörden noch umgesetzt und der DSS nachgewiesen.

«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 Datenschutzaufsichtsbehörden 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 Abschluss der Datenschutzüberprüfungen aus dem Vorjahr

Die im Vorjahr begonnenen amtswegigen Datenschutzüberprüfungen konnten im Berichtsjahr abgeschlossen werden. Im Falle eines Unternehmens, welches sich den Anweisungen der DSS im Rahmen des Prüfverfahrens mit Nachdruck widersetzte, verhängte die DSS eine Geldbusse im Sinne des Art. 83 DSGVO. Im Zuge des Rechtsmittelverfahrens wurde die Geldbusse allerdings von der Beschwerdekommission für Verwaltungsangelegenheiten (VBK) aufgrund verfahrensrechtlicher Erwägungen aufgehoben. Im Hinblick auf die festgestellten Mängel wurde die Verfügung der DSS von der VBK allerdings vollumfänglich bestätigt und das Unternehmen kam zwischenzeitlich den Anweisungen der DSS nach.

5.1.2 Amtswegige Überprüfung: Videoüberwachung in Supermärkten

Wie bereits im Vorjahr wurde die amtswegige Durchführung von Datenschutzüberprüfungen auch im Berichtsjahr fortgesetzt, diesmal jedoch mit Fokus auf Videoüberwachungssysteme in Supermärkten.

Die DSS lancierte diese umfassenden Datenschutzüberprüfungen von Videoüberwachungssystemen in Supermärkten bzw. grösseren Lebensmittelgeschäften am 24. August 2020. Noch nach alter Rechtslage bewilligte Systeme wurden gemäss Art. 89 DSG von den Prüfverfahren ausgenommen. Die Verantwortlichen wurden in diesen Fällen jedoch auf die nach neuer Rechtslage geltende Meldepflicht nach Ablauf ihrer Bewilligung hingewiesen. In acht Fällen leitete die DSS gemäss Art. 58 Abs. 1 DSGVO formelle Prüfverfahren wegen nicht gemeldeter Videoüberwachungsanlagen in Supermärkten ein. Die Verantwortlichen wurden am 24. August 2020 zur Stellungnahme aufgefordert, das heisst zur Übermittlung von Lageplänen mit Standortmarkierungen, Informationen betreffend den Fokusbereich, Screenshots der verwendeten Kameras, Fotos der verwendeten Hinweisschilder bzw. Piktogramme und zur Beantwortung eines umfassenden Fragenkatalogs. Insbesondere wurde um Angaben zum Zeitpunkt der Inbetriebnahme, der Betroffenenkreise, der Rechtsgrundlagen und Verhältnismässigkeitsabwägungen ersucht. Mitte November 2020 lagen der DSS dann die zur Erstellung der Prüfberichte erforderlichen Informationen vor. In einem Fall betreibt der Verantwortliche gemäss Rückmeldung keine Videoüberwachungsanlage, weshalb das diesbezügliche Prüfverfahren eingestellt wurde. In den übrigen sieben Fällen wurden von der DSS die jeweiligen Prüfberichte erstellt und den Verantwortlichen im Dezember 2020 übermittelt.

Zusammengefasst stellte die DSS in den meisten Fällen fest, dass die eingesetzten Videoüberwachungssysteme aus datenschutzrechtlicher Sicht mangelhaft waren. Die Gründe hierfür lagen überwiegend in der oftmals flächendeckenden Überwachung der gesamten Geschäfts- bzw. Ladenfläche, einschliesslich der Kassenzonen, und auch in der von den Verantwortlichen festgelegten, unverhältnismässigen Speicherdauer der Aufnahmen von bis zu 90 Tagen. Diese überschritt die im Normalfall zulässige Speicherdauer von 72 Stunden jeweils deutlich. Als datenschutzrechtlich Betroffene waren Kundinnen und Kunden, Mitarbeitende sowie Lieferanten zu ermitteln. Aufgrund der meist flächendeckenden Videoüberwachung waren insbesondere Mitarbeitende in nicht zumutbarer Weise betroffen, da ihnen kaum mehr ein überwa-

chungsfreier Rückzugsbereich verblieb. Die Verantwortlichen stützten die Videoüberwachungsanlagen in rechtlicher Hinsicht auf Art. 6 Abs. 1 Bst. f DSGVO und führten Diebstahlsprävention bzw. Beweissicherung im Falle von Vermögensdelikten als ihr überwiegendes berechtigtes Interesse an. Vielfach entsprachen die von den Verantwortlichen angebrachten Hinweisschilder und Piktogramme jedoch ebenfalls nicht den gesetzlichen Vorgaben.

Den Verantwortlichen wurde bis Mitte Februar 2021 Gelegenheit eingeräumt, eine abschliessende Stellungnahme abzugeben und allfällige Ergänzungen oder Klarstellungen bei der DSS einzubringen. Auf Grundlage der sohin festgestellten Sachverhalte wird die DSS bei allfälligem Handlungsbedarf von ihren weiteren Abhilfebefugnissen gemäss Art. 58 Abs. 2 DSGVO im Wege rechtsmittelfähiger Verfügungen Gebrauch machen und demgemäss die Prüfverfahren betreffend Videoüberwachungen in Supermärkten 2021 abschliessen können.

5.1.3 Meldung von Videoüberwachungssystemen

Seit Totalrevision des DSG und Inkrafttreten der revidierten Fassung am 1. Januar 2019 unterliegen Videoüberwachungssysteme gemäss Art 5 Abs. 7 DSG nur noch einer Meldepflicht an die DSS (ausgenommen sind lediglich Systeme ohne Aufzeichnungs- oder weitere Verarbeitungsmöglichkeit). Auf die bis anhin geltende Bewilligungspflicht für Videoüberwachungssysteme wurde mit Totalrevision des Gesetzes verzichtet. Mit Stand 17. Dezember 2020 wurden in Liechtenstein insgesamt 85 Videoüberwachungsanlagen (darunter auch Wildtierkameras und Drohnenflüge) gemeldet. Noch nach alter Rechtslage erteilte Bewilligungen wurden jeweils für 5 Jahre erteilt. Im Berichtsjahr erloschen weitere 50 von vormals insgesamt 171 erteilten Bewilligungen. 55 noch aufrechte Bewilligungen erlöschen in den Folgejahren 2021 bis 2023.

5.1.4 Amtswegige Überprüfung: Amt für Gesundheit

Im Spätherbst wurde die DSS von Privatpersonen auf das mit der Corona-Pandemie in Zusammenhang stehende «Contact Tracing» des Amtes für Gesundheit (AG) aufmerksam gemacht. Bei einer ersten informellen Vorabprüfung ist in Zusammenhang mit der Kontaktdatenerhebung insbesondere die fehlende Datenschutzerklärung aufgefallen. Sehr schnell entschied die DSS dann, die bis dahin aus einem Gefüge von Sensibilisierung und Aufsicht bestehende Kooperation mit dem Verantwortlichen für diesen speziellen Fall in eine formelle Datenschutzüberprüfung umzuwandeln. Der Prüfungsumfang wurde so eingeschränkt, dass gezielt einzelne Punkte kontrolliert werden konnten, jedoch das Tagesgeschäft des AG, insbesondere des «Contact Tracing»-Teams, nicht beeinträchtigt wurde. Im Rahmen der datenschutzrechtlichen Überprüfung stellte die DSS folgendes fest:

- Vorab einer jeden umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten (z.B. von Gesundheitsdaten) ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (Art. 35 Abs. 3 Bst. b DSGVO). Seit dem 3. März 2020 wurden im Rahmen des «Contact Tracing» besondere Kategorien personenbezogener Daten vom AG verarbeitet. Eine DSFA wurde jedoch erst über zwei Monate nach der ersten Datenverarbeitung durchgeführt. Weiters musste die DSS feststellen, dass die durchgeführte DSFA wegen mehrerer Mängel nicht als DSFA im Sinne von Art. 35 DSGVO zu qualifizieren war. Eine DSFA ist Ausdruck des risikobasierten Ansatzes der DSGVO. Soweit eine Datenverarbeitung hohe Risiken für die Rechte und Freiheiten natürlicher Personen beinhaltet, sollen diese mithilfe der DSFA vorab identifiziert werden, um sie durch geeignete Schutzmassnahmen technischer wie organisatorischer Art von Anfang an vermeiden bzw. eindämmen zu können. Mit der vorliegend durchgeführten DSFA wurde jedoch keine annähernd zufriedenstellende Risikobeurteilung vorgenommen, wodurch der eigentliche Zweck einer DSFA nicht erfüllt war.
- Der Informationspflicht nach Art. 13 DSGVO bei der Erhebung der personenbezogenen Daten (Datenschutzerklärung) wurde bis zum Abschluss der Überprüfung nicht nachgekommen. So wurden die Betroffenen zum Beispiel nicht darüber informiert, ob und an wen ihre Daten übermittelt werden, wie lange sie gespeichert werden oder ob eine Bereitstellung der personenbezogenen Daten gesetzlich vorgeschrieben ist. Im Rahmen einer fairen und transparenten Verarbeitung müssen Betroffene zudem über ihre Rechte aufgeklärt werden. Die Informationspflicht ist ein zentrales Element des Datenschutzes, denn erst durch sie erlangen betroffene Personen einen Ein- und Überblick, welche Daten zu welchem Zweck über sie verarbeitet werden, und nur so können sie ihre weiteren Rechte wahrnehmen.
- Im Rahmen des «Contact Tracing» wurden seit dem 13. Mai 2020 systematisch mittels eines Erhebungsbogens umfangreiche personenbezogene Daten und insbesondere auch sensible Gesundheitsdaten erhoben. Zur Übermittlung der

Daten wurde ausschliesslich auf die Möglichkeit eines E-Mailversands verwiesen. Das Versenden von E-Mails im Klartext stellt jedoch eine unsichere Art der Kommunikation dar und ist für die Übermittlung von sensiblen und umfangreichen personenbezogenen Daten ungeeignet. Der solchermassen ungeeignete Übermittlungsweg blieb jedoch bis zum Ende der Berichtsperiode bestehen, wodurch dem AG von den Betroffenen ca. 2'000 Erhebungsbögen über einen unsicheren Kommunikationsweg zur Verfügung gestellt wurden. Die DSS musste daher auch eine Verletzung von Art. 5 Abs. 1 Bst. f, Art. 25 und Art. 32 DSGVO feststellen.

– Weiters wurde seit dem 2. Juli 2020 vom AG eine Software zur Bearbeitung des «Contact Tracing» eingesetzt. Ein Drittanbieter agierte diesbezüglich als Auftragsdatenverarbeiter, doch wurde kein nach Art. 28 Abs. 3 DSGVO notwendiger Vertrag mit ihm abgeschlossen.

Die inhaltliche datenschutzrechtliche Überprüfung wurde noch im Berichtsjahr durch die DSS abgeschlossen. Der Verantwortliche hat folgend noch die Möglichkeit zur Stellungnahme, bevor das Verfahren formell abgeschlossen werden wird. Die DSS möchte jedoch trotz der diversen, oben aufgeführten Feststellungen die allgemein gute und kooperative Zusammenarbeit mit dem AG betonen wie auch dessen Bestreben, den Anweisungen der DSS nach Erhalt der Verfügung zügig nachzukommen.

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 der Internetseite im Abschnitt Services ein elektronisches Beschwerdeformular an.

Im Berichtsjahr erhielt die DSS insgesamt 63 Beschwerden von Privatpersonen. 10 dieser 63 Beschwerden wurden von Personen aus anderen EWR-Staaten gegen Verantwortliche in Liechtenstein eingebracht. Eine Beschwerde wurde von einem Bürger in Liechtenstein gegen ein Unternehmen in Grossbritannien eingebracht und von der DSS an die federführende Behörde in Grossbritannien weitergeleitet. 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 etwa 35 % über der Anzahl des Vorjahres.

Auch im Berichtsjahr 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. Ebenfalls ein Thema war die Frage der Geeignetheit von technischen und organisatorischen Massnahmen.

Die DSS machte von ihren Befugnissen unter Art. 58 Abs. 2 DSGVO weitreichend Gebrauch und sprach Verwarnungen, Anweisungen, Beschränkungen und Verbote aus. Geldbussen wurden zwei verhängt, von denen eine in Rechtskraft erwachsen ist und den Betrieb einer Videoüberwachung betraf, während die zweite von der VBK auf Grundlage von Art. 40 Abs. 6 DSG aufgehoben wurde. Die Höhe der Geldbussen war von der DSS relativ tief angesetzt worden und belief sich in beiden Fällen auf einen Betrag von durchschnittlich CHF 4'500.

Die sehr strenge Auslegung der VBK des Art. 40 Abs. 6 DSG lässt der DSS in Zukunft wenig Spielraum, da die VBK trotz des darin zweifach genannten und nicht abschliessenden Kriteriums «insbesondere» feststellt, 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 jede der Sanktionen gemäss Art. 83 und 84 DSGVO «wirksam, verhältnismässig und abschreckend» sein. Bei sehr schwerwiegenden und weitreichenden Verstössen wäre diese Vorschrift aber mit einem generellen Verzicht auf Geldbussen bei erstmaligen Verstössen kaum einzuhalten.

Nicht in jedem 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 und Kunde einer Handelsplattform für Kryptowährungen begehrte Zugriff auf seine personenbezogenen Daten, d.h. den gesperrten Nutzeraccount auf der Webseite der Handelsplattform, und die anschliessende Löschung seiner Daten. Der Nutzeraccount war von der Handelsplattform gesperrt und dem Beschwerdeführer während drei Monaten kein Zugriff darauf gewährt worden. Es stellte sich die Frage, inwieweit der Beschwerdeführer ein Recht auf Zugriff auf sein Konto geltend machen und eine Löschung der Daten begehren kann.
Das Begehren des Beschwerdeführers, auf die im Kunden-Account abgespeicherten personenbezogenen Daten zugreifen zu können, war nach rechtlicher Würdigung der DSS vom Recht auf Datenübertragbarkeit gemäss Art. 20 Abs. 1 DSGVO erfasst. Dieses vermittelt dem Beschwerdeführer als Betroffenem den Anspruch, jene personenbezogenen Daten, die er der Handelsplattform bereitgestellt hat, «in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten». Die Voraussetzungen zur Geltendmachung des Rechts auf Datenübertragbarkeit lagen vor, da die Datenverarbeitung der Handelsplattform auf vertraglicher Grundlage (Nutzervertrag) beruht und die Datenverarbeitung mithilfe automatisierter Verfahren erfolgt. Der Nutzeraccount stellt bereits eine elektronische Kopie der (personenbezogenen) Daten dar, die zur Erbringung der wesenstypischen Dienstleistungen auf einer elektronischen Handelsplattform notwendig sind. Das Recht auf Datenübertragbarkeit kam daher im Beschwerdefall einem faktischen Zugangsrecht auf das (gesperrte) Nutzerkonto gleich. Denn die betreffenden Daten sind (im Einzelfall) in einem schon existierenden Format (hier dem Nutzeraccount) zur Verfügung zu stellen. Im Ergebnis wurde die Handelsplattform angewiesen, dem Beschwerdeführer unverzüglichen Zugang zu seinem Kunden-Konto zu gewähren und den Nutzeraccount zu entsperren. Es handelte sich zudem um keinen Fall, in dem ein Verdacht auf Geldwäscherei etc. das Sperren des Kontos rechtfertigte.

Hinsichtlich des geltend gemachten Löschungsbegehrens gemäss Art. 17 DSGVO wurde der Beschwerde nicht stattgegeben. Die Handelsplattform ist als sorgfaltspflichtiges Unternehmen gemäss Art. 20 Abs. 1 und Art. 20a Abs. 1 und 4 SPG iVm Art. 27 SPV zur Aufbewahrung der Geschäftskorrespondenz und personenbezogenen Daten für eine Dauer von zehn Jahren nach Beendigung der Geschäftsbeziehung oder nach Abwicklung der letzten («gelegentlichen») Transaktion verpflichtet. Dieser Zeitraum war offenkundig noch nicht verstrichen.

Ein Beschwerdeführer machte geltend, dass er Newsletter einer öffentlichen Stelle erhalten habe, ohne sich jemals selbst dafür angemeldet zu haben. Es stellte sich die Frage, ob ein einfaches Opt-in für den Versand eines E-Mail-Newsletters durch eine öffentliche Stelle genügt.
Der Beschwerde betreffend die Verletzung von Art. 5 Abs. 1 Bst. a iVm Art. 6 Abs. 1 DSGVO wurde stattgegeben und festgestellt, dass zum Zeitpunkt der Beschwerdeeinbringung durch den Beschwerdeführer die Verarbeitung personenbezogener Daten durch den Beschwerdegegner aufgrund des Fehlens einer Rechtfertigung gemäss Art. 5 Abs. 1 Bst. a DSGVO iVm Art. 6 Abs. 1 Bst. a und Art. 7 DSGVO aufgrund mangelhafter Einwilligung unrechtmässig war.

Es wurde ebenso festgestellt, dass zum Zeitpunkt der Beschwerdeerhebung eine Verletzung von Art. 5 Abs. 1 Bst. f iVm Art. 32 DSGVO vorlag, die im Laufe des Verfahrens seitens des Beschwerdegegners durch Implementierung des Double-Opt-in-Verfahrens beseitigt wurde. Das Double-Opt-in-Verfahren stellt eine geeignete Massnahme nach Art. 32 DSGVO zur Einholung einer wirksamen Einwilligung für einen elektronischen Newsletter dar. Dabei wird zunächst die E-Mail-Adresse bei der Anmeldung zum Newsletter angegeben («Opt-in»). Dann wird an die angegebene Adresse eine Bestätigungsmail gerichtet, die nur vom tatsächlichen Inhaber dieser E-Mail-Adresse abgerufen werden kann. Wird die Bestätigung erteilt («Double-Opt-in»), wird an die betreffende E-Mail-Adresse ab diesem Zeitpunkt ein Newsletter versandt. Durch das Double-Opt-in wird ausgeschlossen, dass eine dritte Person unbefugt weitere Personen ohne deren Einwilligung zu einem elektronischen Newsletter anmelden kann.

Ein Beschwerdeführer machte geltend, dass er ein Werbeschreiben einer ihm zu diesem Zeitpunkt unbekannten Firma erhalten hat. Es stellte sich die Frage, ob ein ehemaliger Mitarbeiter im Namen seines neuen Arbeitgebers Werbeschreiben an Kunden seines ehemaligen Arbeitgebers versenden darf.
Ein solches Vorgehen kann nicht durch die berechtigten Interessen im Sinne des Art. 6 Abs. 1 Bst. f DSGVO gerechtfertigt werden, da die vernünftigen Erwartungen des Beschwerdeführers insbesondere durch seine konkrete Beziehung zum Beschwerdegegner definiert

werden und es sich im vorliegenden Fall nicht um einen Bestandskunden, sondern einen Neukunden aus Sicht des Beschwerdegegners handelt. Bei Bestandskunden kann grundsätzlich davon ausgegangen werden, dass sie mit Werbung für ähnliche Produkte und Dienstleistungen eines Unternehmens, bei dem sie schon Kunde sind, rechnen müssen. Dies insbesondere dann, wenn sie gemäss Art. 13 DSGVO bereits über die Verwendung ihrer Kundendaten für bestimmte Werbezwecke informiert wurden. Der Beschwerdeführer als potentieller Neukunde des Beschwerdegegners hingegen musste vernünftigerweise nicht mit Werbeschreiben des Beschwerdegegners rechnen. Im vorliegenden Fall hätte es jedenfalls einer expliziten Einwilligung des Beschwerdeführers bedurft, da andernfalls sein Interesse am Schutz vor unerwünschter Werbung überwiegt. Die vom Beschwerdegegner vorgenommene Werbung in Form des persönlichen Werbeschreibens ist somit unrechtmässig im Sinne von Art. 6 Abs. 1 DSGVO.

Ein Beschwerdeführer machte geltend, dass sein ehemaliger Arbeitgeber unrechtmässig auf seinen beruflichen E-Mail-Account zugegriffen hat. Es stellten sich die folgenden Fragen: Bedeutet ein Fehlen interner Reglemente betreffend die Nutzung des beruflichen E-Mail-Accounts für private Zwecke, dass eine solche Privatnutzung automatisch untersagt ist? Kann das langjährige Dulden der privaten Nutzung durch den Arbeitgeber als Erlaubnis einer solchen Nutzung eingestuft werden? Muss ein Arbeitgeber einem ausgeschiedenen Mitarbeitenden Gelegenheit geben, private E-Mails aus dem beruflichen E-Mail-Account zu löschen? Darf der ehemalige Arbeitgeber trotz Widerspruch auf den E-Mail-Account nach Ausscheiden des Arbeitnehmers zugreifen?

Einhergehend mit den Ausführungen in der Orientierungshilfe der deutschen Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz vom Juni 2016 ging die DSS davon aus, dass ein Dulden durch den Arbeitgeber als Erlaubnis einer privaten Nutzung zu werten ist, zumal dem Arbeitgeber im vorliegenden Fall die private Nutzung zweifelsfrei bekannt war.

Ob ein Arbeitgeber auf den E-Mail-Account seiner Mitarbeitenden zugreifen darf, hängt unter anderem vor allem davon ab, ob der Arbeitgeber den Mitarbeitenden die private Nutzung erlaubt oder nicht. Private E-Mail-Korrespondenz betrifft in der Regel die schützenswerte Privatsphäre des jeweiligen Mitarbeitenden. Der Mitarbeitende darf deshalb bei erlaubter oder geduldeter Privatnutzung darauf vertrauen, dass der Arbeitgeber seine Privatsphäre respektiert und in diese nicht rechtswidrig eingreift.

Hinzu kommen die folgenden Faktoren: (i) der Beschwerdegegner kann sich auf einen Rechtfertigungsgrund im Sinne des Art. 6 Abs. 1 DSGVO stützen, (ii) im Fall, dass sich der Beschwerdegegner auf seine berechtigten Interessen im Sinne des Art. 6 Abs. 1 Bst. f DSGVO stützt, wurde eine Interessensabwägung durchgeführt, die ein Überwiegen der Interessen des Beschwerdeführers ausschliesst, (iii) dem Beschwerdeführer wurde Gelegenheit gegeben, seine privaten Daten aus dem E-Mail-Postfach zu löschen, (iv) im Falle des Widerspruchs gemäss Art. 21 DSGVO wurde eine weitere, strengeren Anforderungen unterliegende Interessensabwägung durchgeführt, (v) der Grundsatz der Verhältnismässigkeit und Datenminimierung gemäss Art. 5 Abs. 1 Bst. c DSGVO wurde gewahrt.

Im vorliegenden Fall war vor allem der Punkt (iv) von der DSS detailliert zu prüfen: Hierzu war auszuführen, dass mehrfache Rückmeldungen des Beschwerdeführers als Widerspruch im Sinne des Art. 21 DSGVO zu werten waren. Wie ausgeführt, kann der Zugriff auf ein E-Mail-Postfach grundsätzlich vom Arbeitgeber auf Art. 6 Abs. 1 Bst. f DSGVO gestützt werden, allerdings hat die betroffene Person in diesem Fall ein Widerspruchsrecht gemäss Art. 21 DSGVO. Gemäss Erwägungsgrund 69 sollte der für die Verarbeitung Verantwortliche in einem solchen Fall darlegen, dass seine zwingenden berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Der Prüfungsmassstab ist im Falle des Widerspruchs somit höher anzusetzen als bei einer erstmaligen Abwägung der Interessen bei Berufung auf Art. 6 Abs. 1 Bst. f DSGVO.

Des Weiteren folgt aus der Einlegung des Widerspruchs, dass die betroffene Person das Recht hat, von der verantwortlichen Stelle nach Massgabe des Art. 18 Abs. 1 Bst. d DSGVO das Einstellen der weiteren Verarbeitung ihrer Daten zu verlangen, solange keine Entscheidung über das Überwiegen der zwingenden schutzwürdigen Gründe des Verantwortlichen vorliegt. Der Beschwerdegegner führte gegenüber der DSS aus, dass sein berechtigtes Interesse am Zugriff aufgrund der anstehenden Prüfungen durch die interne und externe Revisionsstelle gegeben sei. Gegenüber dem Beschwerdeführer nannte der Beschwerdegegner als sein berechtigtes Interesse hingegen nur eine «dringliche Angelegenheit». Eine Konkretisierung im Sinne des Art. 21 DSGVO und eine Beschreibung bzw. der Nachweis des Überwiegens der zwingenden berechtigten Interessen erfolgte nicht. Somit konn-

te es nicht als erwiesen angesehen werden, dass der Beschwerdegegner mit der Einsicht in den E-Mail-Account des Beschwerdeführers tatsächlich zwingende Interessen oder die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen verfolgte. Wenn dies der Fall gewesen wäre, wäre es seine Verpflichtung gewesen, den entsprechenden Nachweis zu erbringen.

Ein Beschwerdeführer stellte den Einsatz von Microsoft-Tools im Schulbereich in Frage und beanstandete die Rechtsgrundlage sowie die fehlende Information. Es stellten sich die Fragen, ob der Einsatz digitaler Lehrmittel im Schulbereich zulässig ist und welche Voraussetzungen dafür erfüllt sein müssen. Grundsätzlich ist der Einsatz digitaler Lehrmittel im Schulbereich aus datenschutzrechtlicher Sicht zulässig. Wie bei jeder Datenverarbeitung muss diese Verarbeitung allerdings auf einer Rechtsgrundlage im Sinne des Art. 6 Abs. 1 DSGVO beruhen und es müssen auch alle anderen Grundsätze des Datenschutzrechts eingehalten werden. Als Rechtsgrundlage kommt neben der Einwilligung auch die Erfüllung einer gesetzlichen Vorgabe in Frage. Diese Frage hat der Verantwortliche unmissverständlich zu klären und den betroffenen Personen klar zu kommunizieren. Die Information gemäss Art. 13 DSGVO ist gerade in Bereichen, in denen Kinder und ihre Erziehungsberechtigten die betroffenen Personen sind, besonders wichtig. Daten von Kindern gelten als besonders schützenswert und die Verantwortlichen haben dies bei der Ausgestaltung der Datenverarbeitung entsprechend zu berücksichtigen.

5.2.2 Beschwerden von «NOYB» im Anschluss an das EuGH-Urteil «Schrems II»

Mit dem Urteil in der Rechtssache «Schrems II» erging am 16. Juli 2020 eine der wohl prominentesten Entscheidungen des EuGH in jüngster Zeit mit immenser Bedeutung für den internationalen Datentransfer. In Folge eines Rechtsstreits zwischen dem österreichischen Datenschutzaktivisten Maximilian Schrems und der irischen Niederlassung von Facebook, einem Tochterunternehmen der U.S.-amerikanischen Hauptniederlassung, wurde der sogenannte «EU-U.S.-Privacy-Shield»-Angemessenheitsbeschluss vom EuGH für ungültig erklärt. Dieser Angemessenheitsbeschluss sollte gemäss Art. 45 DSGVO ein angemessenes Schutzniveau für aus dem EU/EWR-Raum in die Vereinigten Staaten übermittelte personenbezogene Daten sicherstellen. Nach eingehender Prüfung des EuGH war jedoch kein angemessenes, dem EU/EWR-Raum gleichwertiges Datenschutzniveau in den Vereinigten Staaten zu erkennen. Gegen die umfassenden – unter anderem im FISA («Foreign Intelligence Surveillance Act») und E.O 12333 («Executive Order») verankerten – Zugriffsrechte der U.S.-Nachrichtendienste besteht für betroffene Personen aus dem EU/EWR-Raum kein hinreichender, gerichtlich durchsetzbarer und wirksamer Rechtsschutz. Betroffene einer Datenübermittlung haben keine Möglichkeit «mittels eines Rechtsbehelfs Zugang zu den (sie) betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken». Eine Übermittlung personenbezogener Daten in die Vereinigten Staaten kann daher seit 16. Juli 2020 nicht länger auf einen entsprechenden Angemessenheitsbeschluss gemäss Art. 45 DSGVO gestützt werden.[5] Eine Übermittlung auf Grundlage von Standarddatenschutzklauseln oder anderer geeigneter Garantien gemäss Art. 46 DSGVO ist grundsätzlich zwar weiterhin denkbar, aber kritisch zu überprüfen.

Über den vorliegenden Fall hinaus ist die Entscheidung des EuGH für sämtliche Datentransfers in Drittstaaten bedeutsam.

Die Datenschutzplattform «NOYB» (ein Akronym für «non of your business») brachte nach Aufhebung des EU-U.S.-Privacy-Shield insgesamt 101 Beschwerden bei europäischen Aufsichtsbehörden ein. Davon richteten sich auch drei Beschwerden gegen Institutionen mit Niederlassung in Liechtenstein. Beanstandet wurde die Datenübermittlung in die Vereinigten Staaten durch Verwendung von Google Analytics und Facebook Connect auf den Webseiten der verantwortlichen Institutionen. Die bei der DSS eingebrachten Beschwerden wurden im Ergebnis jedoch zurückgezogen, da die verantwortlichen Institutionen gegenüber dem Beschwerdeführer NOYB nachweisen konnten, dass die unzulässigen Code-Elemente entfernt wurden und somit keine weitere unrechtmässige Datenübermittlung in die Vereinigten Staaten erfolgte.[6] Mit diesem Vorgehen bildeten die Liechtensteiner Institutionen jedoch die Ausnahme, denn keine der verbleibenden 98 Institutionen, gegen die eine NOYB-Beschwerde eingebracht wurde, reagierte und brachte die Datenverarbeitung bzw. -übermittlung in Einklang mit dem Urteil des EuGH.

Zur Behandlung der Beschwerden wurde zudem eine Arbeitsgruppe des Europäischen Datenschutzausschusses eingerichtet, um ein einheitliches Vorgehen sicherzustellen. An diesen Arbeitsgruppensitzungen nimmt auch die DSS teil. Dies hat trotz des Rückzugs der genannten Beschwerden den Vorteil, dass die DSS

[5] EuGH 16.7.2020, C-311/18 *(Schrems II)* Rz 187.
[6] https://noyb.eu/de/update-zu-noybs-101-beschwerden-ueber-eu-us-datentransfer (abgerufen am 27.4.2021).

über die weiteren Entwicklungen in diesem Zusammenhang in Europa informiert ist und im Fall weiterer Beschwerden wegen Datenübermittlungen in Drittstaaten diese bei der Durchführung nationaler Verfahren berücksichtigen kann.

5.2.3 Urteil des EFTA-Gerichtshofes in der Rechtssache E-11/19 und E-12/19 (Adpublisher AG ./. J und Adpublisher AG ./. K)

In zwei Beschwerdefällen erhob das verantwortliche Unternehmen als ursprünglicher Beschwerdegegner 2019 gegen die Entscheidungen der DSS Beschwerde an die VBK. Diese legte in den beiden gleich gelagerten Fällen zwei Rechtsfragen dem EFTA-Gerichtshof (EFTA-GH) vor, der sie in der Folge miteinander verband.

Am 10. Dezember 2020 veröffentlichte der EFTA-GH seine vielerwartete Entscheidung zur verbundenen Rechtssache E-11/19 und E-12/19. In den strittigen Verfügungen hatte die DSS über zwei Datenschutzbeschwerden wegen behaupteter Verletzungen von Art. 5, 6 und 15 DSGVO, die im Zusammenhang mit dem Adresshandel der Adpublisher AG als Verantwortlicher standen, entschieden. In den gegenständlichen Beschwerden an die DSS wünschten die Beschwerdeführer, dass sie im Verfahren und vor allem gegenüber dem Beschwerdegegner anonym blieben. Die DSS prüfte diese Anliegen und stellte fest, dass die Anonymität den Verfahren nicht entgegenstünden. Die Beschwerde führenden Personen blieben folglich auch im Verfahren vor der VBK anonym, obwohl der Beschwerdegegner eine Offenlegung der Identität der Beschwerdeführer verlangte. Über die von den Beschwerdeführern geltend gemachten Verletzungen der Datenschutzbestimmungen hinaus erkannte die DSS in einem Fall amtswegig einen Verstoss gegen Art. 7 und 32 DSGVO durch die Adpublisher AG.

Die VBK legte dem EFTA-GH in der Folge zwei Vorlagefragen zur Zulässigkeit der Anonymität von Beschwerdeführenden sowie zur Kostenersatzpflicht in Beschwerdeverfahren vor weiterführenden Rechtsmittelinstanzen gemäss Art. 78 DSGVO zur Vorabentscheidung vor. Es ging konkret darum zu klären, ob Beschwerdeverfahren gemäss Art. 77 und 78 Abs. 1 DSGVO durchgeführt werden dürfen, ohne dass die Identität der Beschwerdeführer offengelegt wird. Falls eine solche Anonymisierung zulässig wäre, sei fraglich, ob hierfür eine sachliche Rechtfertigung erforderlich wäre oder zumindest glaubhaft dargelegt werden müsse.

Eine weitere Vorlagefrage bezog sich darauf, ob ein Mitgliedstaat in seinem nationalen Verfahrensrecht sicherstellen müsse, dass im Beschwerdeverfahren gemäss Art. 77 DSGVO alle weiteren nationalen Rechtsmittelinstanzen für die betroffene Person unentgeltlich sind und ein Kostenersatz nicht auferlegt werden dürfe.

Der EFTA-GH stellte zur Klärung der ersten Vorlagefrage in bemerkenswerter Deutlichkeit klar, dass jegliche Datenverarbeitung – also auch die Offenlegung von personenbezogenen Daten durch eine Aufsichtsbehörde – nur zulässig ist, wenn sie rechtmässig erfolgt und den Datenschutzgrundsätzen entspricht. Das gilt auch für die Aufsichtsbehörde (DSS) und die Rechtsmittelinstanz (VBK), die als Verantwortliche für die Verarbeitung personenbezogener Daten von Beschwerdeführern zu qualifizieren sind. Eine grundsätzliche Offenlegungspflicht wurde vom EFTA-GH nicht erkannt, vielmehr ist die die Offenlegung von Daten Beschwerdeführender etwa daran zu messen, ob diese Angaben erforderlich sind, um Anweisungen der DSS nachzukommen. Vielfach ist eine Kenntnis der Identität des Beschwerdeführers nicht nötig, wenn eine standardisierte und gleichartige Datenverarbeitung eine unbestimmte Anzahl von Personen oder mehrere gleichartige Beschwerden betrifft. Nur wo eine Kenntnis durch den Beschwerdegegner für die wirksame Ausübung seines Verteidigungsrechts absolut erforderlich ist, muss ihm die Identität des Beschwerdeführers offengelegt werden.

Zur fraglichen Kostenersatzpflicht im Beschwerdeverfahren gemäss Art. 78 Abs. 1 DSGVO stellte der EFTA-GH klar, dass sie dem Recht auf eine unentgeltliche Beschwerde entgegensteht. Wenn einer betroffenen Person, die kein Verfahren nach Art. 78 Abs. 1 DSGVO einleitet, ohne deren Zutun der Status einer Beklagten (d.h. Verfahrenspartei) zugewiesen wird, «würde sich die potenzielle Auferlegung von Kostenersatz so auswirken, als würde eine Gebühr für die Aufgaben der Aufsichtsbehörde verlangt.» Die Aussicht auf Kostenersatzpflicht kann vor der Einreichung einer Beschwerde abschrecken und lässt sich mit der Ratio der DSGVO, die einen einfachen und kostenlosen Rechtsschutz gewährleisten möchte, nicht vereinbaren. Das entgegenstehende nationale Verfahrensrecht hat folglich unangewendet zu bleiben. Im Beschwerdeverfahren gemäss Art. 78 Abs. 1 DSGVO vor der VBK darf folglich einer Person, die (ohne ihr Zutun) zur Verfahrenspartei wurde, keine Kostenersatzpflicht auferlegt werden.

5.3 Meldung von Datenschutzverletzungen gemäss Art. 33 DSGVO

Art. 33 DSGVO sieht vor, dass Verletzungen des Schutzes personenbezogener Daten der zuständigen Datenschutzaufsichtsbehörde binnen 72 Stunden zu melden sind, wenn aufgrund der Verletzung voraussichtlich ein Risiko für die Rechte und Freiheiten na-

türlicher 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.

Im Berichtsjahr erhielt die DSS 20 Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO, wovon in sieben Fällen die betroffenen Personen über die Datenschutzverletzung benachrichtigt wurden (Art. 34 DSGVO). Die Meldungen zeigten, 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 in einem weiteren Schritt zu einem späteren Zeitpunkt nachgeliefert werden. Die Meldungen erfolgten von Banken, Versicherungen, Telekommunikationsbetrieben, Gewerbe und Treuhandunternehmen.

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.

«Die DSS unterstützte die Regierung bei der Schaffung der entsprechenden Rechtsgrundlagen durch eine intensive Beteiligung an der Ausarbeitung des revidierten Gesetzes.»

6. Mitarbeit in Arbeitsgruppen und Projekten der Landesverwaltung

6.1 Gesetzesrevisionen Steuerverwaltung

Im Berichtsjahr wurde die DSS von der Steuerverwaltung (STV) zu Rate gezogen bezüglich der datenschutzrechtlichen Aspekte mehrerer geplanter Gesetzesrevisionen, und zwar des Gesetzes über den internationalen automatischen Informationsaustausch in Steuersachen (AIA-Gesetz), des Gesetzes über die Umsetzung des FATCA-Abkommens zwischen dem Fürstentum Liechtenstein und den Vereinigten Staaten von Amerika (FATCA-Gesetz), des Gesetzes zum Abkommen zwischen Liechtenstein und Österreich über die Zusammenarbeit im Bereich der Steuern (AStA-Gesetz) und des Gesetzes über den internationalen automatischen Austausch länderbezogener Berichte multinationaler Konzerne (CbC-Gesetz).

Die DSS war dabei einerseits beratend tätig bei der konkreten, DSGVO-konformen Formulierung der entsprechenden Passagen in den revidierten Gesetzen und im Vernehmlassungsbericht wie auch im Bericht und Antrag an den Landtag. Ausserdem begleitete die DSS die STV bei der Abstimmung der neu gefassten datenschutzbezogenen Regelungen mit den diversen Anspruchsgruppen aus der Finanzwelt.

6.2 Ratifikation Konvention 108+

Die DSS hat im Berichtsjahr ausserdem das Amt für Auswärtige Angelegenheiten (AAA) 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 hat die DSS daher massgeblich zur Erarbeitung des Regierungsantrags zur Unterzeichnung des Änderungsprotokolls beigetragen und war bereits in vorbereitende Arbeiten für den Bericht und Antrag an den Landtag involviert. Die formelle Ratifikation des Änderungsprotokolls durch Liechtenstein wird für 2021 erwartet.

6.3 Zentrales Personenregister

Das Zentrale Personenregister (ZPR) wurde Ende der Neunzigerjahre in der Landesverwaltung eingeführt und seither laufend ausgebaut. Die zentral geführte Datenbank wird von zahlreichen Amtsstellen genutzt und enthält unter anderem Daten sämtlicher Einwohnerinnen und Einwohner Liechtensteins und Daten von im Ausland wohnhaften Personen, die mit der Landesverwaltung in Kontakt getreten sind. Sie stellt daher ein besonders wichtiges Arbeitsinstrument der Landesverwaltung dar. Bereits 2017 wurden seitens der Regierung erste Aufgabenpakete für eine Modernisierung des ZPR beschlossen.

Neben technischen Aspekten, die bei der Neugestaltung des ZPR in Bezug auf den Datenschutz zu berücksichtigen sind und die vor allem im Vorjahr diskutiert wurden, stellten sich im Berichtsjahr zahlreiche datenschutzrechtliche Fragen bei der (Total-) Revision des Gesetzes über das Zentrale Personenregister (ZPRG). Die DSS unterstützte die Regierung bei der Schaffung der entsprechenden Rechtsgrundlagen durch eine intensive Beteiligung an der Ausarbeitung des revidierten Gesetzes.

6.4 Projekt Elternportal (cse.kibe)

Sowohl im Vorjahr als auch im Berichtsjahr wurde die DSS mehrfach zu Rate gezogen vom Ministerium für Gesellschaft, vom Amt für Soziale Dienste und vom Amt für Informatik (AI) bezüglich datenschutzrechtlicher Aspekte bei der Einführung einer zentralen Abrechnungsplattform für staatlich subventionierte Kinderbetreuungseinrichtungen. Die DSS unterstützte dabei einerseits die Ausgestaltung der Internetseite und der Datenbank in Bezug auf eine Begrenzung der Datenverarbeitung auf das absolut erforderliche Mass sowie in Bezug auf die Zuweisung der (begrenzten) Benutzerrechte. Andererseits begleitete die DSS die Ausarbeitung eines Auftragsverarbeitungsvertrags mit dem Schweizer Dienstleister, die Entwicklung einer umfassenden Datenschutzinformation für die betroffenen Eltern auf dem so genannten Elternportal, sowie die Gewährleistung eines hohen Niveaus an Datensicherheit auf der entwickelten Internetseite und Datenbank. Betreffend die Datensicherheit wurden gemeinsam mit dem AI mehrere Gespräche mit dem Lieferanten geführt. Bei einer Sicherheitsüberprüfung konnten zahlreiche Schwachstellen erkannt werden, welche schliesslich durch den Lieferanten behoben wurden. Ebenso wurde zwischen dem AI und dem Lieferanten eine Vorgehensweise vereinbart, der die Datensicherheit auch zukünftig auf dem geforderten hohen Niveau gewährleistet. Die DSS begleitete die Gespräche und stand unterstützend zur Seite. Auch mit den betroffenen Kinderbetreuungseinrichtungen wurde an umfassenden und zugleich leicht verständlichen Daten-

schutzinformationen für die Eltern wie auch für das Betreuungspersonal gearbeitet, die jenen Teil der Datenverarbeitung betreffen, der nach wie vor direkt vor Ort in den Kinderbetreuungseinrichtungen stattfindet.

6.5 Datenschutz-Folgenabschätzung bei der SFIU

Die Stabsstelle Financial Intelligence Unit (SFIU) ist die zentrale Behörde zur Beschaffung und Analyse von Informationen, die zur Erkennung von Geldwäscherei, Vortaten der Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung notwendig sind. Zudem nimmt die SFIU verschiedene Vollzugsaufgaben wie beispielsweise die Entgegennahme von Meldungen im Zusammenhang mit beschlossenen internationalen Sanktionen wahr. Bei den damit zusammenhängenden Datenverarbeitungen handelt es sich um solche, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben. Eine Abschätzung der Folgen der Verarbeitungsvorgänge für den Schutz personenbezogener Daten (Datenschutz-Folgenabschätzung) war somit notwendig. Die DSS unterstützte die SFIU insbesondere in der Anfangsphase bei der Erfassung und Beschreibung der Verarbeitungsvorgänge. In weiterer Folge sollten anhand der geplanten oder bereits vorhandenen Sicherheitsmassnahmen mit einer Risikobeurteilung allfällige Risiken und Schwachstellen erkannt und minimiert bzw. beseitigt werden. An dieser Stelle übernahm die Datenschutzbeauftragte der LLV die Beratung, wobei die DSS für Fragen weiterhin zur Verfügung stand.

«Europäisches Fazit: Weder die DSGVO noch die nationalen Datenschutzgesetze verhindern Massnahmen zur Bekämpfung der Covid-19-Pandemie, zeigen aber klare Grenzen auf.»

7. Internationale Zusammenarbeit

7.1 Europäischer Datenschutzausschuss

Eine der Hauptaufgaben des Europäischen Datenschutzausschusses (EDSA) ist der Erlass von Leitlinien, die der Auslegung der DSGVO dienen (EDPB Guidelines). Die Grundlagen für die Leitlinien des Ausschusses werden in insgesamt zwölf thematischen Arbeitsgruppen «Expert Subgroups» geschaffen, welche die Dokumente für die Abstimmung im Ausschuss vorbereiten. Erstmalig war es für die DSS – nicht zuletzt aufgrund der nun guten Personalsituation – möglich, an den meisten Sitzungen der Arbeitsgruppen teilzunehmen und dort, wo es für Liechtenstein von Bedeutung ist, aktiv mitzuarbeiten. Wie wohl alle Bereiche prägte die Pandemie ab März des Berichtsjahres auch den EDSA und seine Arbeit. Aufgrund des dringenden Bedarfs zahlreicher Interessensgruppen an Leitlinien im Zusammenhang mit der Verarbeitung von Personendaten in der Pandemie wurde die Frequenz der Plenarsitzungen des EDSA deutlich erhöht. Von vormals einer Plenarsitzung pro Monat in Brüssel traf sich der EDSA beispielsweise im April und Mai des Berichtsjahres bis zu zwei Mal wöchentlich per Telefon- oder Videokonferenz. Die DSS nahm an sämtlichen 25 Plenarsitzungen im Berichtsjahr teil. Dem EDSA sowie der DSS war und ist es ein wichtiges Anliegen darauf hinzuweisen und zu betonen, dass die Datenschutzbestimmungen – weder jene der DSGVO noch diejenigen der nationalen Datenschutzgesetze – Massnahmen zur Bekämpfung der Covid-19-Pandemie verhindern.

Im Berichtsjahr hat der EDSA auf Grundlage des Art. 64 Abs. 1 DSGVO insgesamt 31 Stellungnahmen abgegeben und dabei folgende Themenbereiche behandelt:

- 11 Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Überwachung von Verhaltensregeln gemäss Art. 41 DSGVO (Spanien, Belgien, Frankreich, Deutschland, Irland, Finnland, Italien, Niederlande, Dänemark, Griechenland, Polen);
- 10 Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Zertifizierung gemäss Art. 43 Abs. 3 DSGVO (Grossbritannien, Luxemburg, Irland, Deutschland, Tschechien, Niederlande, Griechenland, Italien, Dänemark, Österreich);
- eine Stellungnahme zum Entwurf der Standardvertragsklauseln gemäss Art. 28 Abs. 8 DSGVO (Slowenien);
- 9 Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (FAE Group, zwei zur Reinsurance Group of America, Jotun, Tetra Pak, Iberdrola Group, Equinix, Coloplast Group, Novelis Group).

Zusätzlich verfasste der EDSA gemäss Art. 64 Abs. 2 DSGVO eine Stellungnahme zu nationalen Listen über Verarbeitungstätigkeiten, die keiner Datenschutz-Folgenabschätzung unterliegen (Frankreich).

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

- Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen (EDPB Guidelines 01/2020);
- Übermittlungen personenbezogener Daten zwischen Behörden und Einrichtungen des EWR und ausserhalb des EWR gemäss Art. 46 Abs. 2 lit. a und Abs. 3 lit. b DSGVO (EDPB Guidelines 02/2020);
- Verarbeitung von Gesundheitsdaten zum Zweck der wissenschaftlichen Forschung im Zusammenhang mit dem COVID-19-Ausbruch (EDPB Guidelines 03/2020);
- Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 (EDPB Guidelines 04/2020);
- Einwilligung gemäss Verordnung 2016/679 (EDPB Guidelines 05/2020);
- Zusammenspiel der zweiten Zahlungsdienste-richtlinie und der DSGVO (EDPB Guidelines 06/2020);
- Konzepte des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters in der DSGVO (EDPB Guidelines 07/2020);
- Targeting von Social-Media-Nutzern (EDPB Guidelines 08/2020);
- Erheblicher und begründeter Einwand gemäss Verordnung 2016/679 (EDPB Guidelines 09/2020);
- Beschränkungen gemäss Art. 23 DSGVO (EDPB Guidelines 10/2020).

Zwei Empfehlungen wurden zu folgenden Themen angenommen:

- Massnahmen zur Ergänzung von Übermittlungsinstrumenten, um die Einhaltung des EU-Schutz-

niveaus für personenbezogene Daten zu gewährleisten (EDPB Recommendations 01/2020);
– Europäische Grundlegende Garantien für Überwachungsmassnahmen (EDPB Recommendations 02/2020).

7.1.1 Arbeitsgruppen

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. 2020 wurde von der Arbeitsgruppe die Arbeit an offiziellen Leitlinien des EDSA dazu aufgenommen, welche die Berechnung von Bussgeldern methodisch systematisieren und europaweit harmonisieren sollen. Die Arbeiten daran sind bereits weit fortgeschritten und sollen 2021 abgeschlossen werden.

In der Arbeitsgruppe, die sich mit der Zusammenarbeit der Aufsichtsbehörden befasst *(Cooperation Subgroup)*, wurde im Berichtsjahr speziell mit der Ausarbeitung der Leitlinien des EDSA zum Kooperationsverfahren bei grenzüberschreitenden Beschwerden gemäss Art. 60 DSGVO begonnen. Die Arbeit daran erforderte intensive Diskussionen und Konsensbemühungen seitens aller Mitgliedstaaten, ist doch ein harmonisierter europäischer Prozess zu schaffen, der dennoch Raum für sämtliche involvierten nationalen Verfahrensrechte lässt. Eine Verabschiedung dieser wichtigen Leitlinien wird 2021 erwartet.

Diejenige Arbeitsgruppe des EDSA, welche sich mit der möglichst einheitlichen Durchsetzung der Bestimmungen der DSGVO in den Mitgliedstaaten befasst *(Enforcement Subgroup)*, war im Berichtsjahr zum ersten Mal mit der Durchführung eines Streitbeilegungsmechanismus gemäss Art. 65 DSGVO beschäftigt. Mehrere betroffene Aufsichtsbehörden hatten massgeblichen und begründeten Einspruch gegen den Beschlussentwurf einer federführenden Aufsichtsbehörde eingelegt, dem sich diese jedoch nicht angeschlossen bzw. den diese abgelehnt hatte. Der in solchen Fällen erforderliche verbindliche Beschluss des EDSA zur Streitbeilegung wurde von der Arbeitsgruppe vorbereitet. Ausserdem wurden von der Arbeitsgruppe 2020 Leitlinien zum massgeblichen und begründeten Einspruch verfasst und die Arbeit an generellen Leitlinien zum Verfahren des Streitbeilegungsmechanismus gemäss Art. 65 DSGVO aufgenommen. Die Verabschiedung letzterer Leitlinien wird ebenfalls 2021 erwartet.

Die thematische Arbeitsgruppe des EDSA zu Finanzangelegenheiten *(Financial Matters Subgroup)* hat im Berichtsjahr insbesondere die Leitlinien zum Zusammenspiel der überarbeiteten europäischen Zahlungsdiensterichtlinie (PSD2) und der DSGVO fertiggestellt, welche im Dezember 2020 nach Abschluss des öffentlichen Konsultationsverfahrens vom EDSA formell verabschiedet wurden. Des Weiteren hat diese Arbeitsgruppe 2020 kleinere Beiträge zu Themen wie FATCA, Kryptowährungen, Speicherung von Kreditkartendaten, Bekämpfung von Geldwäscherei und Terrorismusfinanzierung erarbeitet.

Die Arbeitsgruppe zu Fragen bezüglich Datenübermittlungen in Drittstaaten *(International Transfer Subgroup)* hat im Berichtsjahr die Vorbereitungen für eine Richtlinie zur Nutzung von Verhaltensregeln (Codes of Conduct) wie auch Zertifizierungen als geeignete Garantien für internationale Datentransfers aufgenommen. Eine klare Lösung in dieser komplexen Fragestellung konnte allerdings noch nicht erarbeitet werden. Weiters bemühte sich die Arbeitsgruppe auch 2020 um eine bessere Strukturierung und Koordination von BCR-Verfahren («Binding Corporate Rules» bzw. «verbindliche interne Datenschutzvorschriften»). Aufgrund bisheriger Erfahrungen und Rückmeldungen wurde eine Überarbeitung der zur Verfügung gestellten Hilfestellungen («Working-Papers») in Angriff genommen. Regelmässig auftretende Unklarheiten sollen spezifiziert, wie auch uneinheitliche Anwendungen und Interpretationen der Aufsichtsbehörden aus dem Weg geräumt werden. Auch Brexit und die Konsequenzen des Schrems II-Urteils des EuGH wurden in der Arbeitsgruppe besprochen und Beiträge und Unterstützung beispielsweise in Form von Stellungnahmen des EDSA vorbereitet.

Die CEH-Arbeitsgruppe, 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, die nachfolgend zur Stellungnahme an den EDSA gehen sollten. Im Berichtsjahr standen naturgemäss auch verstärkt gesundheitsbezogene Themen in Bezug auf COVID-19 und deren datenschutzrechtliche Implikationen auf der Tagesordnung der Sitzungen der CEH-Arbeitsgruppe.

Die Arbeitsgruppe *Technology* befasste sich im Jahr 2020 mit einem breiten Spektrum an Fragestellungen in Kooperation mit internationalen Gremien wie beispielsweise der Europäischen Regulierungsstelle für elektronische Kommunikation (BEREC) sowie der Agentur der Europäischen Union für Cybersicherheit

(ENISA), der Aus- und Überarbeitung von Leitlinien bzw. Empfehlungen sowie die Beantwortung verschiedener Fragen von Mitgliedern des europäischen Parlaments. Konkrete Leitlinien wie beispielsweise zu Art. 25 DSGVO zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen oder zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen wurden im Jahr 2020 veröffentlicht. Im Zusammenhang mit dem Schrems II-Urteil wurden Empfehlungen ausgearbeitet zu zusätzlichen Massnahmen, welche die Einhaltung des EWR-Schutzniveaus für personenbezogene Daten bei einem Drittstaat-Transfer gewährleisten sollen. Diese Empfehlungen wurden am 11. November 2020 in die öffentliche Konsultation gegeben. Bis zur Eingabefrist am 21. Dezember wurden über 200 Kommentare eingereicht.

Im Fokus der Arbeitsgruppe *Social Media* stand die Fertigstellung der Richtlinie für das Targeting von Social-Media-Nutzern. Da die öffentliche Konsultationsphase am 19. Oktober endete, wird mit der verabschiedeten Version erst Anfang 2021 zu rechnen sein. Neben den Richtlinien für das Targeting befinden sich weitere Richtlinien in Ausarbeitung, die voraussichtlich ebenfalls im 2021 angenommen und veröffentlicht werden. Unter anderem wird an einem Leitfaden zum Datenschutz an den Schnittstellen von Social Media Plattformen gearbeitet. Dabei sollen Hilfestellungen zum Design von Social Media Plattformen und zur Vermeidung von trügerischen Design-Unarten, den sogenannten «Dark Patterns», in der Praxis dargeboten werden. Die Empfehlungen beruhen auf einer interdisziplinären Schnittstellenanalyse, die auch verhaltenswissenschaftliche Aspekte einbezieht.

Die Arbeitsgruppe BTLE *(Border Travel and Law Enforcement)* befasste sich im Berichtsjahr unter anderem mit der Polizei-Richtlinie (EU) 2016/680 (RL). Die Polizeirichtlinie (EU) 2016/680 RL regelt die Verarbeitung personenbezogener Daten für Behörden, die für die Verhütung, Ermittlung, Aufdeckung oder für die Verfolgung von Straftaten zuständig sind. Insbesondere wurden Berichte ausgearbeitet, die einen Überblick über die internationale Datenübermittlung im Bereich der Strafverfolgung und Erfahrungen bei der Datenübermittlung vorbehaltlich geeigneter Garantien betreffend den Austausch von polizeilichen Daten mit Drittländern aufzeigen. Des Weiteren wurden im Berichtsjahr Leitlinien für die Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses nach Art. 36 und 37 RL zur Beschlussfassung vorbereitet. Die Arbeitsgruppe hat zudem eine Stellungnahme zum Zusatzprotokoll zum Übereinkommen über Computerkriminalität verfasst, an der Ausarbeitung der EDSA-Empfehlungen zu den Europäischen Grundlegenden Garantien für Überwachungsmassnahmen mitgewirkt, als auch an den Empfehlungsentwürfen für ergänzende Massnahmen sowie den Auswirkungen von Schrems II mitgearbeitet. Im Weiteren hat die Arbeitsgruppe die Möglichkeit genutzt, die Richtlinie zur Gesichtserkennung und die rechtliche Studie über Drittländer zu kommentieren.

Das *DPO-Network* ist ein auf europäischer Ebene angesiedeltes Netzwerk der für die Datenschutzaufsichtsbehörden der europäischen Mitgliedstaaten amtierenden Datenschutzbeauftragten. Ziel dieses Netzwerkes ist die Bildung von Know-how sowie der Erfahrungsaustausch unter den Datenschutzbeauftragten und die Erleichterung ihrer Arbeit durch Schaffung gleicher Standards. Über dieses primäre Ziel hinaus widmet sich das DPO-Network den ihm durch den EDSA zugewiesenen spezifischen Themen, so auch im Berichtsjahr (z.B. Analyse des Einsatzes von Twitter als Kommunikationsmedium).

7.1.2 Gegenseitige Amtshilfe

Wie eingangs erwähnt, erfordert die DSGVO nicht nur eine Zusammenarbeit im bzw. mit dem EDSA, sondern auch eine intensive Kommunikation zwischen den einzelnen europäischen 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». Seit Geltung der DSGVO in Liechtenstein am 20. Juli 2018 ist die DSS daher gemäss Art. 61 DSGVO zur gegenseitigen Amtshilfe verpflichtet. Hierbei handelt es sich um eine neue und zusätzliche Aufgabe, die der DSS mit Inkrafttreten der DSGVO erwachsen ist. Die DSS erhielt im Berichtsjahr 41 Anfragen von anderen europäischen Datenschutzaufsichtsbehörden, was im Vergleich zu den im Vorjahr beantworteten 23 Anfragen erneut eine starke Zunahme bedeutete. Die Anfragen wurden jeweils gestellt, wenn im Vollzug der aufsichtsrechtlichen Tätigkeit Interpretationsspielraum bestand und die anfragende Datenschutzaufsichtsbehörde die Rechtsmeinung anderer Aufsichtsbehörden bzw. die Anwendung von Bestimmungen der DSGVO durch andere Mitgliedstaaten erfahren wollte. Die Anfragen betrafen unter anderem Fragen zur Verarbeitung von biometrischen Daten durch Banken und Finanzinstitutionen, Gesichtserkennung, Videoüberwachung und angemessene Aufbewahrungsfristen der Bilddaten, automatisierte Entscheidungsfindung oder Datenverarbeitung im Rahmen der Geldwäschereiprävention.

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.

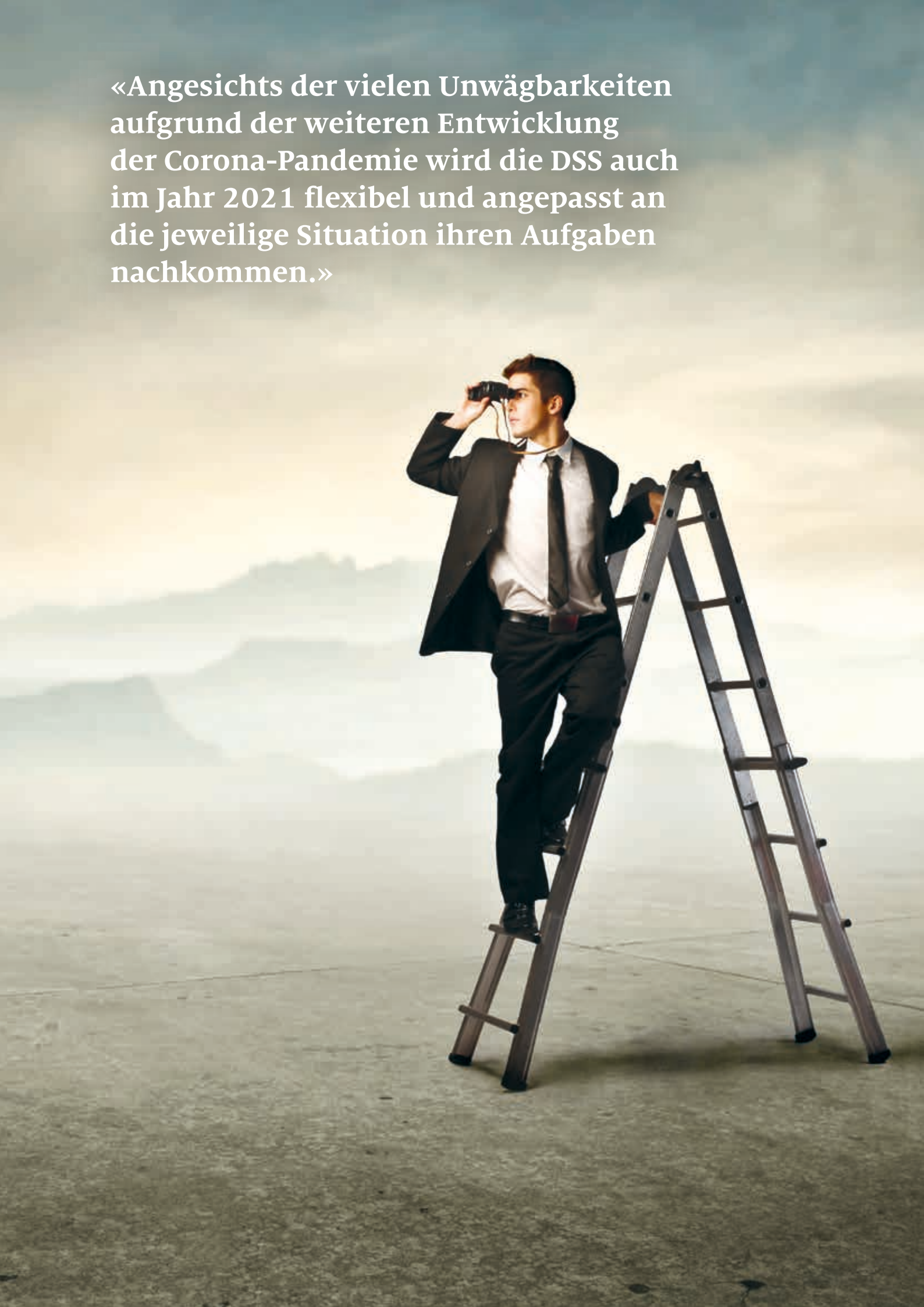
7.2 Europarat

Die DSS hat im Jahr 2020 erneut an diversen virtuellen Arbeitssitzungen sowie an der 40. Versammlung des Beratenden Ausschusses des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) des Europarats teilgenommen. Letztere Veranstaltung fand aufgrund der Corona-Pandemie erst im November statt und wurde ebenfalls nur virtuell durchgeführt.

Der Beratende Ausschuss der Konvention 108 hat sich im Berichtsjahr zunächst ebenfalls intensiv mit der Corona-Pandemie und dem Zusammenspiel von Datenschutz und diversen staatlichen Bekämpfungsmassnahmen befasst. Auf Basis einer breiten Umfrage unter den Mitgliedstaaten wurde der Bericht «Digital solutions to fight COVID-19» veröffentlicht. Daneben bestand die Hauptarbeit des Beratenden Ausschusses aber weiterhin in der Erarbeitung von Berichten, Positionspapieren u.ä. zu den Themen Gesichtserkennung, Datenschutz im Bildungswesen, Datenschutz in politischen Kampagnen und Wahlen, Digitale Identitäten, Profiling sowie grenzüberschreitender Zugang zu Daten in der Strafverfolgung. Die Ergebnisse können zu künftigen Handlungsempfehlungen, Leitfäden, Resolutionen oder Erklärungen auch übergeordneter Organe des Europarates führen. So hat der Ministerrat im April 2020 etwa eine Empfehlung zum Einfluss algorithmischer Systeme auf Menschenrechte verabschiedet («Recommendation on the human rights impacts of algorithmic systems»).

Die Konvention 108 wurde kürzlich mittels eines Änderungsprotokolls modernisiert und insbesondere an die heutigen informations- und kommunikationstechnologischen Möglichkeiten der Datenverarbeitung angepasst. Die DSS unterstützt das Amt für Auswärtige Angelegenheiten beim entsprechenden Ratifikationsprozess durch Liechtenstein. Im Berichtsjahr hat die DSS massgeblich zur Erarbeitung des Regierungsantrags zur Unterzeichnung des Änderungsprotokolls beigetragen, welcher von der Regierung am 10. November 2020 beschlossen wurde und zur offiziellen Unterzeichnung des Änderungsprotokolls am 7. Dezember 2020 in Strassburg führte. Die formelle Ratifikation des Änderungsprotokolls durch Liechtenstein wird für 2021 erwartet.

«Angesichts der vielen Unwägbarkeiten aufgrund der weiteren Entwicklung der Corona-Pandemie wird die DSS auch im Jahr 2021 flexibel und angepasst an die jeweilige Situation ihren Aufgaben nachkommen.»



8. Schlussbemerkung und Ausblick

Wenngleich das Jahr 2020 und auch der Datenschutz sehr stark von der Corona-Pandemie geprägt waren, darf nicht übersehen werden, dass diese vielen zusätzlichen Fragestellungen, welche durch die Pandemie entstanden und von der DSS, aber auch den anderen europäischen Datenschutz-Aufsichtsbehörden beantwortet werden mussten, nicht all die anderen alltäglichen Datenschutzfragen ersetzten, sondern sich zusätzlich zu diesen stellten. Damit waren in diesem Jahr grosse Herausforderungen zu bewältigen gewesen. Hinzu kam, dass die DSS selbst ebenfalls die Umstellung auf das Home-Office und die neue (digitale) Arbeitsweise der europäischen Gremien meistern musste.

Und auch für das Jahr 2021 scheint sich nicht wirklich eine Rückkehr zum Normalmodus abzuzeichnen. Aus diesem Grund umfasst die Veranstaltungs-Planung der DSS für 2021 sowohl Online-Veranstaltungen als auch Vor-Ort-Veranstaltungen. Zu letzteren zählt auch die Weiterführung der Veranstaltungsreihe «Workshops» in Kooperation mit der Privaten Universität. Sobald es die Situation erlaubt, soll etwa ein weiterer Workshop zum Thema «Webauftritt und Datenschutz» stattfinden. Nicht stattfinden wird bedauerlicherweise der Datenschutztag Ende Januar 2021, da hierfür eine Online-Veranstaltung nicht als adäquater Ersatz gewertet werden kann. Hingegen ist es der DSS ein sehr grosses Anliegen, das Vernetzungstreffen für Datenschutzbeauftragte im Herbst 2021 wieder vor Ort durchführen zu können. Die Datenschutzbeauftragten sind verantwortlich für die Umsetzung des Datenschutzes in ihren Unternehmen oder öffentlichen Institutionen und haben sich dabei mit zahlreichen hochkomplexen rechtlichen und technischen Fragen auseinanderzusetzen. Letztlich müssen sie ihre Umsetzungsvorschläge auch gegenüber der jeweiligen Unternehmensleitung vertreten. Die DSS sieht den Austausch mit den Datenschutzbeauftragten daher als einen zentralen Aspekt ihrer Tätigkeit an. Ihre Beratung gewinnt angesichts der technologischen Entwicklungen, der informationellen Globalisierung und des komplexen rechtlichen Rahmens täglich an Bedeutung.

Teil dieses beratungsmässigen Schwerpunkts wird 2021 auch die Beteiligung bzw. Kooperation der DSS an dem von der Universität Liechtenstein geplanten Lehrgang im Datenschutzrecht sein. Mit diesem praxisorientierten Lehrgang sollen vertiefte und anwendungsorientierte Kenntnisse zu den rechtlichen Rahmenbedingungen sowie den technischen Aspekten der Datensicherheit und dem Datenschutzmanagement vermittelt werden. Nachdem auch hier der Austausch und direkte Kontakt mit den Teilnehmenden im Vordergrund steht, wäre natürlich die Durchführung vor Ort die ideale Variante.

Angesichts der vielen Unwägbarkeiten aufgrund der weiteren Entwicklung der Corona-Pandemie wird die DSS auch im Jahr 2021 flexibel und angepasst an die jeweilige Situation ihren Aufgaben nachkommen. Dabei soll auch die Umsetzung spontaner Ideen, wie des im Berichtsjahr im Rahmen von ferienspass.li angebotenen Internet-Surfscheins für Kinder und Jugendliche, weiterhin möglich sein und wird die DSS von aussen an sie herangetragenen Projektideen aufgeschlossen gegenüberstehen.

Datenschutzstelle Fürstentum Liechtenstein
Städtle 38
Postfach 684
FL-9490 Vaduz

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