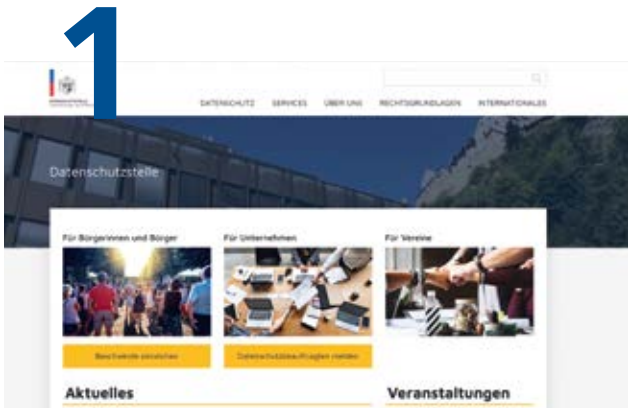
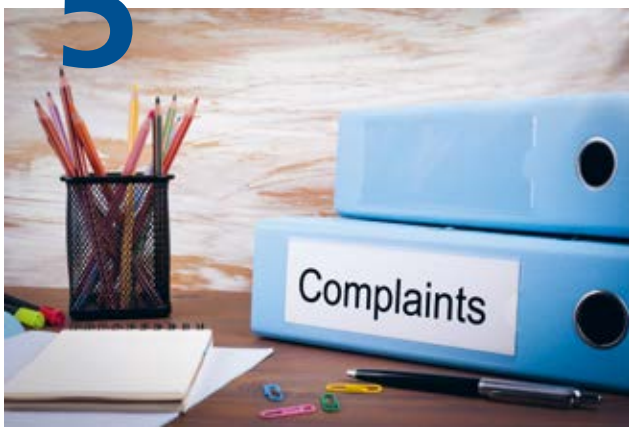
DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

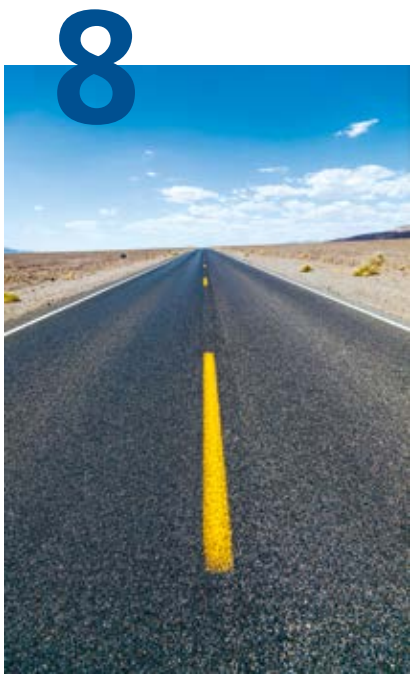
Tätigkeitsbericht Datenschutzstelle
Fürstentum Liechtenstein

Tätigkeitsbericht 2021

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

Nach über drei Jahren Geltung der Datenschutz-Grundverordnung (DSGVO) sowie des liechtensteinischen Datenschutzgesetzes (DSG) sind die meisten öffentlichen und privaten Institutionen mit den grundlegenden Anforderungen im Bereich des Datenschutzes vertraut und haben diese zumindest in Grundzügen umgesetzt. Das bedeutet aber keinesfalls, dass sich damit der Arbeitsaufwand für die Datenschutzstelle (DSS) reduziert hat. Nach wie vor ist es eine herausfordernde Aufgabe, den Datenschutzbestimmungen nachvollziehbar, einheitlich und effektiv zur Umsetzung zu verhelfen. Die Aufgaben der DSS passen sich den jeweiligen Entwicklungen an und konzentrieren sich aktuell vermehrt darauf, zu überprüfen, welche neuen Erkenntnisse, die sich aus der Rechtsprechung in Europa oder den Vorgaben des Europäischen Datenschutzausschusses (EDSA) ergeben, dazu führen, dass Datenverarbeitungsprozesse in Unternehmen und öffentlichen und privaten Stellen angepasst werden müssen. Diese werden dann transparent an die verantwortlichen Stellen kommuniziert. Besondere Aufmerksamkeit wurde dabei im Berichtsjahr den Entwicklungen im Bereich des internationalen Datentransfers geschenkt. Während etwa Google Analytics zu Beginn der Geltung der DSGVO noch als konform eingestuft wurde, begannen die Alarmzeichen nach dem Urteil des Europäischen Gerichtshofs (EuGH) in der Rechtssache «Schrems II» aufzuleuchten, wenngleich als Reaktion darauf in der täglichen Praxis eher vorsichtiges Abwarten die übliche Vorgehensweise bei den meisten datenverarbeitenden Stellen war. Ende des Berichtsjahres gab es dann die erste Entscheidung einer europäischen Aufsichtsbehörde zur Verwendung von Google Analytics. Diese stellte fest, dass die Verwendung von Google Analytics im konkreten Fall nicht datenschutzkonform war. Die DSS informierte über diese Entwicklungen in regelmässigen Abständen und empfahl Verantwortlichen und Auftragsverarbeitern, sich mit dieser Thematik frühzeitig auseinanderzusetzen.

Eine Aktualisierung war auch in Bezug auf zahlreiche weitere Informationen auf der Internetseite der DSS erforderlich. So erfolgten im Berichtsjahr neben weiteren Informationen zum internationalen Datentransfer etwa auch Anpassungen in Bezug auf die Situation in Grossbritannien nach dem Brexit, die neuen Standardvertragsklauseln der EU-Kommission, den Beschäftigtendatenschutz oder die Verwendung von Bild- oder Videoaufnahmen zur Öffentlichkeitsarbeit. Schliesslich sorgten auch die regelmässigen Änderungen der staatlichen Massnahmen zur Covid-19 Bekämpfung dafür, dass die Lage und die getroffenen datenschutzrechtlich relevanten Massnahmen immer wieder neu eingeschätzt und bewertet werden mussten.

Dr. Marie-Louise Gächter, Leiterin Datenschutzstelle

Neben der Beratung, die sich erneut an die unterschiedlichsten Akteure aus dem privaten und öffentlichen Sektor richtete, stand auch die Aufsicht in ihren vielfältigen Ausprägungen auf der Tagesordnung der DSS. Insbesondere die Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde gemäss Art. 33 DSGVO nahmen 2021 stark zu. Die Zahl der Beschwerden hingegen blieb ungefähr im Bereich des Vorjahres und auch die geltend gemachten Verletzungen entsprachen zu einem grossen Teil jenen aus den Vorjahren. Bei den Beschwerdegegnern hielten sich öffentliche und private Stellen knapp die Waage.

Von grosser Bedeutung für die Arbeit der DSS waren auch die vom Verwaltungsgerichtshof (VGH) getroffenen Entscheidungen im Berichtsjahr, welche die Anwendung der geltenden Datenschutzbestimmungen durch die DSS bestätigten. Mit seinen Entscheidun-

gen gab der VGH umfangreiche Antworten sowohl in Bezug auf das materielle Recht, aber auch die anzuwendenden Verfahrensvorschriften. Damit sorgte er für Rechtssicherheit und wichtige Leitlinien für die Arbeit der DSS.

Insgesamt zeigte sich auch 2021 erneut, dass eine transparente, kundenorientierte und kooperative Arbeitsweise der DSS der richtige Ansatz für eine effiziente und effektive Durchsetzung der Datenschutzbestimmungen ist. Eine gewisse Einschränkung erfuhr dieser Ansatz bedauerlicherweise im Berichtsjahr einmal mehr dadurch, dass der direkte Kontakt mit betroffenen Personen ebenso wie mit datenverarbeitenden Stellen nur sehr eingeschränkt möglich war.

Vaduz, im April 2022

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

1. Öffentlichkeitsarbeit

Auch im vierten Jahr ihrer Anwendbarkeit sind noch längst nicht alle Fragen in Bezug auf die DSGVO geklärt. Und auch in Bezug auf das liechtensteinische Datenschutzgesetz (DSG) gibt es nach wie vor Klärungsbedarf. Datenschutz und vor allem seine Umsetzung unterliegen einem steten Wandel, bedingt sowohl durch den technologischen Fortschritt als auch neue Erkenntnisse aus der Rechtsprechung. Der alleinige Blick in den Gesetzestext garantiert somit noch keine perfekte praktische Umsetzung der datenschutzrechtlichen Vorgaben. Ohne eine aktive Informations- bzw. Wissensvermittlung seitens der Aufsichtsbehörden wird Datenschutz nicht die Rolle bei 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, Internetseite und individuelle Beratungen. Insbesondere das Zusammenwirken dieser Kommunikationskanäle ermöglicht es, dass eine sehr grosse Zahl an Adressatinnen und Adressaten erreicht werden kann. Bedauerlicherweise mussten auch im Berichtsjahr wieder zahlreiche Veranstaltungen aufgrund der Covid-19-Beschränkungen abgesagt oder auf kleine Kreise beschränkt werden. In einzelnen Fällen war immerhin ein Ausweichen auf Online-Kanäle möglich. Damit konnte die Öffentlichkeitsarbeit im Berichtsjahr erneut nicht in dem Umfang durchgeführt werden, wie bei der Jahresplanung angestrebt.

1.1 Veranstaltungen

Zum grossen Bedauern der DSS musste der Datenschutztag, der wie üblich jedes Jahr Ende Januar stattfinden sollte, auf Grund der Covid-19-Beschränkungen verschoben werden. Es war geplant, zwei renommierte Referenten zum Thema «Überwachungsstaat» einzuladen, welche die Situation in China beleuchten sowie analysieren sollten, ob der chinesische Ansatz auch in Europa eines Tages zum Einsatz kommen könnte. Im Anschluss war eine Diskussion vorgesehen zur Frage, wie sich Liechtenstein zu einer solch weitreichenden staatlichen Überwachung der Bürgerinnen und Bürger stellt. Nachdem die Fragen der Möglichkeit bzw. Reichweite staatlicher Überwachung wiederholt auch Thema von Anfragen aus der Bevölkerung sind, soll die Veranstaltung im Frühsommer 2022 nachgeholt werden.
Nach der Absage im Vorjahr konnte im Berichtsjahr hingegen am 8. November das Vernetzungstreffen für Datenschutzbeauftragte wieder im Vaduzer Saal stattfinden. Der rege und kontinuierliche Austausch mit den Datenschutzbeauftragten nimmt einen hohen Stellenwert in der Tätigkeit der DSS ein. Denn nur so lässt sich erkennen, wo Aufklärungs- und Unterstützungsbedarf besteht. Ebenfalls ist es ein grosses Anliegen der DSS, dass die Datenschutzbeauftragten einen Einblick in die Tätigkeit der Aufsichtsbehörde erhalten. Insbesondere Informationen zu ergangenen Entscheidungen der DSS sorgen für Rechtssicherheit und Orientierungshilfe. Darüber hinaus wies die DSS auch mit einem kurzen Überblick auf relevante Entscheidungen von Aufsichtsbehörden und Gerichten (vor allem) im deutschsprachigen Ausland hin. Auch wenn die DSS an diese Entscheidungen nicht unmittelbar gebunden ist, doch einer einheitlichen Anwendung des Datenschutzrechts im EU / EWR-Raum, diese Entscheidungen in eigenen Verfahren mit zu berücksichtigen und im Falle einer anderslautenden Entscheidung diese auch nachvollziehbar zu begründen.

Nach dem grossen Erfolg der im Vorjahr neu eingeführten Workshops entschied die DSS, die Workshop-Reihe im Berichtsjahr weiterzuführen und plante ursprünglich Workshops zu drei bis vier unterschiedlichen Themengebieten. Schliesslich war dann aufgrund der Covid-19-Beschränkungen lediglich die Durchführung von Workshops zu einem einzigen Thema möglich. Nachdem bei der DSS im Berichtsjahr vermehrt Anfragen zur korrekten Umsetzung datenschutzrechtlicher Aspekte im Zusammenhang mit der Gestaltung und Umsetzung von Webseiten eingingen, entschied die DSS, die Workshops auf dieses Thema zu konzentrieren. Insbesondere das «Schrems II»-Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 16. Juli 2020 erhöhte die Verunsicherung, was den Einsatz von Social-Media-Plugins, Webtracking, Cookie-Banner usw. betrifft. Um Verantwortlichen, Webentwicklern und allen Interessierten einen Überblick über die unterschiedlichen technischen sowie rechtlichen Rahmenbedingungen und Anforderungen zu vermitteln, führte die DSS im Oktober insgesamt drei Workshops zum Thema «Datenverarbeitung im Zusammenhang mit Webauftritten» durch. Nach einer theoretischen Einführung in das Thema erarbeiteten und diskutierten die Teilnehmenden datenschutzkonforme Ausgestaltungen von Internetseiten anhand konkreter Fallbeispiele. Für den einfachen Einstieg war in einem Fall ein Webauftritt eines Vereins durch die Teilnehmenden in Bezug auf den Datenschutz zu prüfen. Die Annahme war, dass der Verein den Webauf-

tritt auf einem virtuellen Server betreibt, welcher bei einem lokalen Hoster im Land angemietet wurde. Weiters wurde angenommen, dass standardmässig sämtliche zusätzlichen Plug-ins und sonstige Erweiterungen deaktiviert und dynamische Seiten nicht vorhanden sind sowie keine statistischen Daten von Besuchern erhoben werden. In einem weiteren Fall war ein Webauftritt zu prüfen, der wesentlich näher an der Praxis lag und bei dem auch wesentlich mehr Berührungspunkte mit dem Datenschutz vorhanden waren. So wurde etwa angenommen, dass sich der Verantwortliche eines im Ausland befindlichen Webhosters aus dem Internet bedient, welcher über ein Suchportal ausgewählt wurde und die Inhalte über ein vom Hoster zur Verfügung gestelltes CMS gepflegt werden. Dabei konnte mit den Teilnehmenden ein Cookie-Banner, Anforderungen an Newsletter und Kontaktformulare sowie Plug-ins externer Anbieter diskutiert werden. Speziell die Empfehlung zum Einsatz des zur Inspektion von Internetseiten nützlichen Entwickler-Werkzeugs – welches in allen gängigen Browsern vorhanden ist – empfanden die Teilnehmenden dabei als sehr hilfreich. Mit dem Workshop sollte die Kompetenz der Teilnehmenden praxisnah gestärkt werden, die rechtmässige Datenverarbeitung im Kontext von Webauftritten insbesondere 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 mindestens zwei Workshops zu aktuellen Themen anzubieten.

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. Diesen Ansatz verfolgte die DSS auch im Berichtsjahr weiter, wenngleich aufgrund der Covid-Massnahmen leider nur in sehr eingeschränktem Rahmen.

Daher hat sich die DSS aufgrund des grossen Interesses am Angebot der DSS im Rahmen des Projektes «Ferienspass» im Jahr 2020 dazu entschieden, auch im Sommer 2021 wieder an der Aktion «Ferienspass» teilzunehmen. So konnte eine Kindergruppe an einem Nachmittag auf spielerische Art und Weise einen Einblick in Soziale Medien, Online-Spiele und Videoplattformen gewinnen. Dabei wurde in Bezug auf die eigene Bekanntgabe von personenbezogenen Daten beim Surfen oder Spielen im Internet sensibilisiert, aber auch in Bezug auf Influencer, Medien und Werbung in und über soziale Kanäle.

1.2 Vorträge

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

1.2.1 Kooperation mit den Universitäten in Liechtenstein

Auch im Berichtsjahr war die Intention, schwerpunktmässig mit den beiden Universitäten in Liechtenstein zusammenzuarbeiten und gemeinsame Veranstaltungen anzubieten. Aufgrund personeller Änderungen an der Universität Liechtenstein fanden aber mit dieser im Berichtsjahr bedauerlicherweise keine spezifischen gemeinsamen Veranstaltungen im Bereich Datenschutz statt.

Im Rahmen der Veranstaltungsreihe der Privaten Universität im Fürstentum Liechtenstein «FL meets UFL» gab die Leiterin der DSS am 28. Mai einen Einblick in das Thema «Darknet» und beantwortete damit einige grundlegende Fragen: «Was ist das Darknet eigentlich?», «Wie funktioniert das Darknet?», «Wer bewegt sich in dieser unsichtbaren digitalen Welt und wie kann, darf oder soll man in diese Welt eindringen?», «Welche Rolle spielt der Datenschutz im Darknet bzw. welche Rolle spielt das Darknet für den Datenschutz?»

Am 30. November fand an der Privaten Universität zum dritten Mal in Folge eine ganztägige Weiterbildungsveranstaltung zum Thema «Anwendung der DSGVO – Expertenwissen für interessierte Praktiker» statt. Der Vortrag der DSS im Rahmen der online durchgeführten Veranstaltung befasste sich mit dem Thema «Aktuelle Entwicklungen im Internationalen Datentransfer, unter besonderer Berücksichtigung der neuen Standardvertragsklauseln». Dabei stand die Frage im Mittelpunkt, ob mit den neuen Klauseln tatsächlich ein Wandel von dem vom EuGH in der Rechtssache «Schrems II» geforderten Rechte-basierten-Ansatz hin zu einem Risiko-basierten-Ansatz gelungen ist. Auch wenn sich für die DSS noch gewisse Zweifel in Bezug auf diesen Richtungswechsel ergeben, wird die Möglichkeit des verstärkten Praxisbezugs beim internationalen Datentransfer auch bei Prüfungen oder Beratungen der DSS eine Rolle spielen. Nichtsdestotrotz ist die DSS überzeugt, dass die Rechtslage in einem Drittstaat ohne Angemessenheitsbeschluss weiterhin

die Hauptrolle spielen muss und die Frage der Rechtsbehelfe bzw. der Ausübung der Betroffenenrechte ein ausschlaggebendes Kriterium in der Beurteilung der Zulässigkeit des Datentransfers bilden muss.

1.2.2 Weitere Vorträge

Zusätzlich nahmen Mitarbeitende der DSS an 17 Informations- und Diskussionsveranstaltungen als Referentinnen bzw. Referenten teil oder hielten Vorlesungen oder Vorträge an Informations- und Weiterbildungsveranstaltungen, vor allem an der Universität Liechtenstein oder der Privaten Universität im Fürstentum Liechtenstein. Beispielsweise befasste sich die Vorlesung der DSS im Rahmen des LL.M. im Bank- und Finanzmarktrecht im Dezember mit der Frage, ob die DSGVO und DLT-Systeme bzw. Blockchain-Anwendungen miteinander kompatibel sind. Wenig überraschend lautete das Ergebnis, dass diese Frage nach wie vor eine konkrete und abschliessende Antwort vermissen lässt. Die Tatsache, dass praktische Anwendungsfälle noch nicht ausreichend vorhanden sind, erschwert hier ebenfalls die Suche nach präzisen Antworten.

Weiters wirkte die DSS bei verschiedenen, von Unternehmen ausgerichteten Veranstaltungen mit. Im Besonderen leistete die DSS im Berichtsjahr wieder Beiträge bei Veranstaltungen dieser Unternehmen für ihre Lernenden. In Kursen für Gastwirte und Sachbearbeiter / Innen informierte die DSS über die grundlegenden Datenschutz-Anforderungen an einen Betrieb sowie aktuelle Entwicklungen im Bereich Datenschutz. Dazu kam eine Veranstaltung des Privacy-Rings und eine Veranstaltung in Zürich für betriebliche Datenschutzexperten. Diese Veranstaltungen in den Nachbarstaaten standen vor allem im Zeichen der Kooperation der DSS mit Datenschutzbehörden im nahen Ausland sowie dort ansässigen Datenschutzvereinigungen. Gerade mit der Schweiz gibt es zahleiche Anknüpfungspunkte und viele Verantwortliche oder Auftragsverarbeiter in der Schweiz sind entweder direkt der DSGVO unterworfen oder kooperieren mit Unternehmen oder öffentlichen Stellen in Liechtenstein.

1.2.3 Mitarbeiterschulungen

Da aufgrund der Covid-19-Beschränkungen grössere Weiterbildungsveranstaltungen für Unternehmen kaum angeboten werden konnten, nahm die DSS im Berichtsjahr erneut die Einladung von verschiedenen liechtensteinischen Firmen für Mitarbeiterschulungen an. Anfang Jahr führte die DSS etwa eine Präsentation mit anschliessender Fragerunde für mehrere Vermögensverwaltungsfirmen durch. Dabei standen insbesondere die für diese Branche relevanten datenschutzrechtlichen Fragestellungen im Vordergrund. Die Schulung konnte zu diesem Zeitpunkt jedoch leider nur virtuell über ein Videokonferenz-Tool abgehalten werden.

Im Herbst führte die DSS dann wieder vor Ort in einem grossen Treuhandunternehmen eine Mitarbeiterschulung zu datenschutzrechtlichen Fragen durch, welche sich praxisnah an einem typischen Kundenberatungsprozess im Treuhandbereich orientierte. Auch hier konnten viele Fragen zu unterschiedlichen Datenschutzthemen von der DSS beantwortet werden.

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

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 Thema Datenschutz und Covid-19, Informationen zum Schengener Informationssystem, welches von der Landespolizei für die grenzüberschreitende Polizeizusammenarbeit genutzt wird, zu besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) und personenbezogenen Daten zu strafrechtlichen Verurteilungen und Straftaten (Art. 10 DSGVO), zu den neuen Standardvertragsklauseln der EU-Kommission oder den Angemessenheitsbeschlüssen für das Vereinigte Königreich sowie ein Spickzettel zur DSGVO für die Praxis / Technik. Zudem überarbeitete die DSS aufgrund von neuen Entwicklungen in der Praxis, Rechtsprechung oder Leitlinien

des Europäischen Datenschutzausschusses (EDSA) einzelne Themenbereiche und informierte darüber auch mittels Newsletter.

Die Internetseite der DSS mit ihrem breiten Informationsangebot erfreut sich dabei eines ungebrochenen Interesses. Knapp die Hälfte aller Zugriffe auf die Internetseite betreffend die verschiedenen Themen unter der Rubrik «Themen A - Z» wurden bei folgenden Beiträgen verzeichnet: Berechtigtes Interesse, Informationspflicht nach Art. 13 und 14 DSGVO, kleines Konzernprivileg, Datenschutzerklärung für Internetseiten und Cloud-Services.

1.4 Newsletter

Die Zugriffszahlen auf den Newsletter stiegen im Berichtsjahr erneut an. Ende 2021 hatten 1'176 Personen den Newsletter der DSS abonniert. Dies entspricht einem Plus von 63 Abonnenten gegenüber dem Vorjahr. 2021 hat die DSS insgesamt 19 Newsletter versandt.

Die drei meistgelesenen Newsletter 2021 waren der «DSGVO-Spickzettel» für die Praxis / Technik, das Update zum Datenschutz nach dem Brexit sowie jener über die neuen Standardvertragsklauseln der EU-Kommission. Bei der Wahl der Inhalte berücksichtigte die DSS soweit möglich die Bedürfnisse der Adressatinnen und Adressaten und reagierte auf verstärkte Anfragen zu bestimmten Themen.

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

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

1.5 Datenschutz in den Medien

Im Berichtsjahr war der Datenschutz wieder prominent in den liechtensteinischen Medien vertreten. Die Schwerpunkte waren erneut zu einem grossen Teil von der Covid-19-Pandemie bestimmt. Themen der über 50 Berichte in den Printmedien waren neben zahlreichen Berichterstattungen zur Datenverarbeitung im Rahmen von Covid-19-Massnahmen (wie 3G, elektronisches Impfzertifikat etc.) der Austausch von Casino-Sperrlisten, die Familienforschung oder Cyberattacken. Darüber hinaus erschienen auch mehrere Berichte zu den von der DSS gegen das Schulamt erlassenen Verfügungen.

Zudem hat das Volksblatt zusammen mit der DSS im Berichtsjahr eine Reihe von Gastkommentaren initiiert, die sich nicht direkt dem Datenschutz selbst, sondern dem technologischen Umfeld davon widmeten. So erklärte die DSS die technischen Hintergründe beispielsweise von Fingerabdruck-Scannern oder Ge-

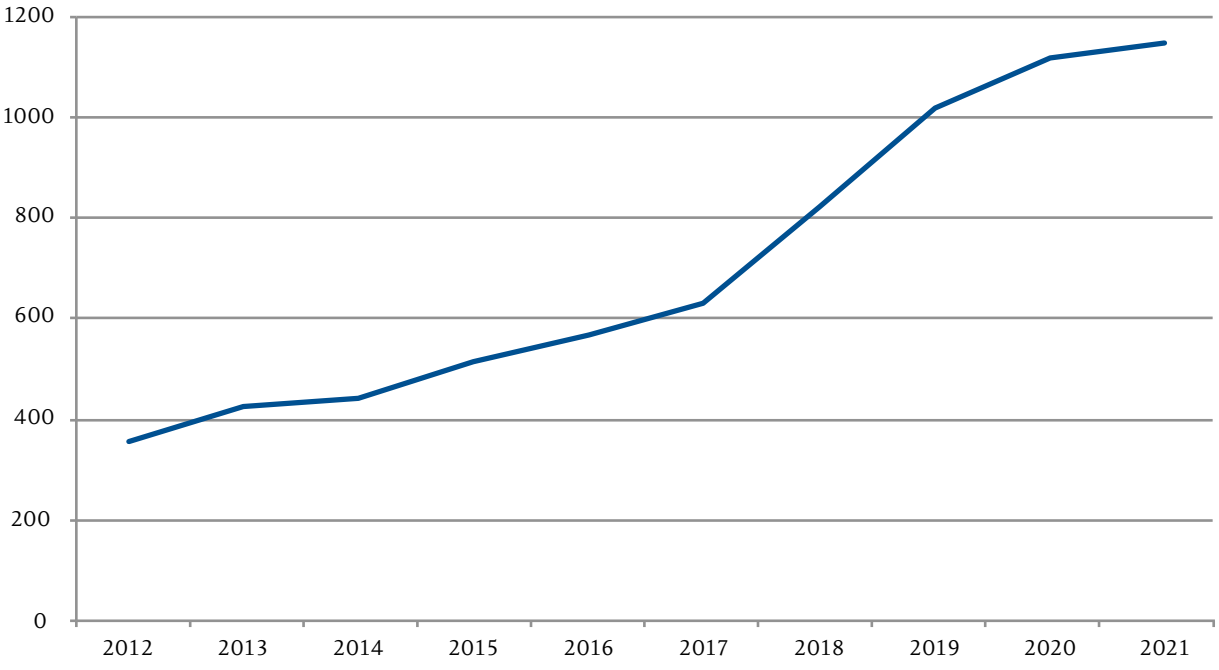


Abbildung 1: Entwicklung Newsletter Abonnentinnen und Abonnenten

sichtserkennungssoftware, dem Darknet, der Cloud, dem Internet der Dinge, künstlicher Intelligenz, Quantencomputern, Cookies, Verschlüsselungstechniken und vielem mehr. Diese Gastkommentare können auch jederzeit auf der Internetseite der DSS im Newsarchiv nachgelesen werden.

Die Berichterstattung zu datenschutzrechtlichen Themen in den Medien sowie deren positive Haltung gegenüber der Materie ist ein wertvoller Beitrag zur Umsetzung des kommunikativen Konzepts der DSS bzw. der Vermittlung datenschutzrechtlicher Themen an die Bevölkerung, da so die Information auch für Bürgerinnen und Bürger greifbar wird, die von Berufswegen weniger Berührungspunkte mit dem Datenschutz haben.

«Privatpersonen machten 13,3 % der Fragestellenden aus und zeigten damit erneut grosses Interesse am Datenschutz.»

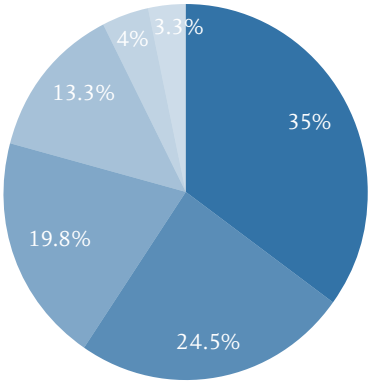
2. Beratung in Bezug auf konkrete Anfragen

2.1 Allgemeines

Im Berichtsjahr verzeichnete die DSS 1'284 Anfragen von öffentlichen und privaten Institutionen sowie Privatpersonen. Im Vergleich zu den im Vorjahr beantworteten 1'544 Anfragen bedeutet dies einen zahlenmässigen Rückgang. Dies wird allerdings kompensiert durch die Komplexität der Anfragen, die gegenüber dem letzten Jahr wie auch im Jahr zuvor deutlich gestiegen ist. Dies war einerseits den vielen Fragen geschuldet, die mit der Covid-19-Pandemie verbunden waren und umfangreichere Evaluationen und Abklärungen erforderten, wie etwa in Bezug auf die Verwendung von 3G am Arbeitsplatz oder ähnlichen Datenverarbeitungen durch Arbeitgeber zur Umsetzung der Covid-19-Schutzmassnahmen. Andererseits zeigte sich, dass der technische Fortschritt zahlreiche neue und herausfordernde Fragen aufwirft, ob und inwieweit die jeweiligen technischen Systeme die Datenschutzanforderungen erfüllen können. So waren etwa bezüglich des Einsatzes von Videoüberwachungsanlagen durch Private oder Unternehmen im Berichtsjahr umfangreiche Beratungstätigkeiten seitens der DSS zu verzeichnen, die wiederum vertiefte Kenntnisse im rechtlichen wie auch technischen Bereich verlangten. Ebenso gab es zahlreiche Anfragen zu den neuen Standard-Vertragsklauseln der EU-Kommission, die seit dem 4. Juni 2021 anwendbar sind und für die Verantwortlichen und Auftragsverarbeiter neben vielen Vorteilen auch zahlreiche Fragen mit sich brachten. Zusätzliche Unsicherheiten bestanden ausserdem nach wie vor in Bezug auf das «Schrems II»-Urteil des EuGH und vor allem betreffend die nachfolgenden Beschwerden von Max Schrems bzw. seiner Datenschutzorganisation noyb zur Frage der Zulässigkeit von Google Analytics oder ähnlichen Analyse-Tools. Auch Fragen zu Cookies sowie der rechtskonformen Ausgestaltung von Cookie-Bannern kamen sehr häufig vor. Insgesamt liess sich zudem feststellen, dass die direkten Anfragen an die DSS zwar zurückgingen, die Zugriffe auf Informationen auf der Internetseite allerdings klar zunahmen.

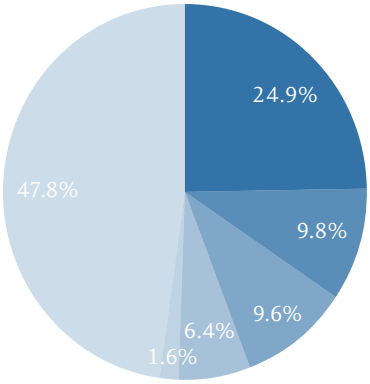
Zur Herkunft der Fragestellenden ist festzuhalten, dass diese dem Trend des letzten Jahres folgend zu einem grossen Teil aus der Privatwirtschaft stammten (35.0 %). Nicht ganz die Hälfte davon wiederum waren kleine und mittlere Unternehmen sowie Kleinstunternehmen. An zweiter und dritter Stelle folgten internationale Akteure (24.5 %) sowie die Behörden von Landesverwaltung und Gemeinden (19.8 %). Privatpersonen machten immerhin 13.3 % der Fragestellenden aus und zeigten damit erneut grosses Interesse am Datenschutz. Die Anfragen von den Medien waren im Berichtsjahr auf dem Niveau des Vorjahres (4.0 %).

Wer stellt die Fragen?



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

Verteilung der Anfragen aus der Privatwirtschaft



- Finanzintermediäre
- Anwaltskanzleien
- Versicherungen
- Gesundheitswesen
- Verbände
- Andere

Beratungsanfragen konnten telefonisch, schriftlich – insbesondere mittels E-Mail – oder auch in einem persönlichen Gespräch bei der DSS eingebracht werden. Von den 1'284 Anfragen wurden im Berichtsjahr lediglich 156 telefonisch gestellt und beantwortet, während 2019 und 2020 noch 413 bzw. 214 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 und 2021 entsprechend die Ausnahme waren.

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

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

2.2 Videoüberwachung und Veröffentlichung von Bildmaterial

Mit Inkrafttreten des DSG erfuhr die Videoüberwachung öffentlich zugänglicher Räume in Art. 5 eine neue gesetzliche Regelung. Wie die DSS in ihren letzten Tätigkeitsberichten erläuterte, nahmen in Folge dessen die Anfragen zur Videoüberwachung stark zu. Dieser Trend hielt auch 2021 weiter an. Videoüberwachungen sind und bleiben ein aktuelles Thema. Es ist klar erkennbar, dass deren Nutzung stetig weiter ausgebaut wird bzw. werden möchte, und dies in allen Bereichen.

Im Rahmen der mit Art. 5 Abs. 7 DSG sowie Art. 5 DSV eingeführten Meldepflicht von Videoüberwachungen öffentlich zugänglicher Räume sind im Berichtsjahr 7 Drohnenflüge und 28 Videoüberwachungsanlagen bei der DSS gemeldet worden.

Bereits im Tätigkeitsbericht 2020 berichtete die DSS, dass in Bezug auf eine seit längerem bestehende Videoüberwachung einer Freizeitanlage einer Gemeinde die Empfehlung seitens der DSS erfolgte, dass

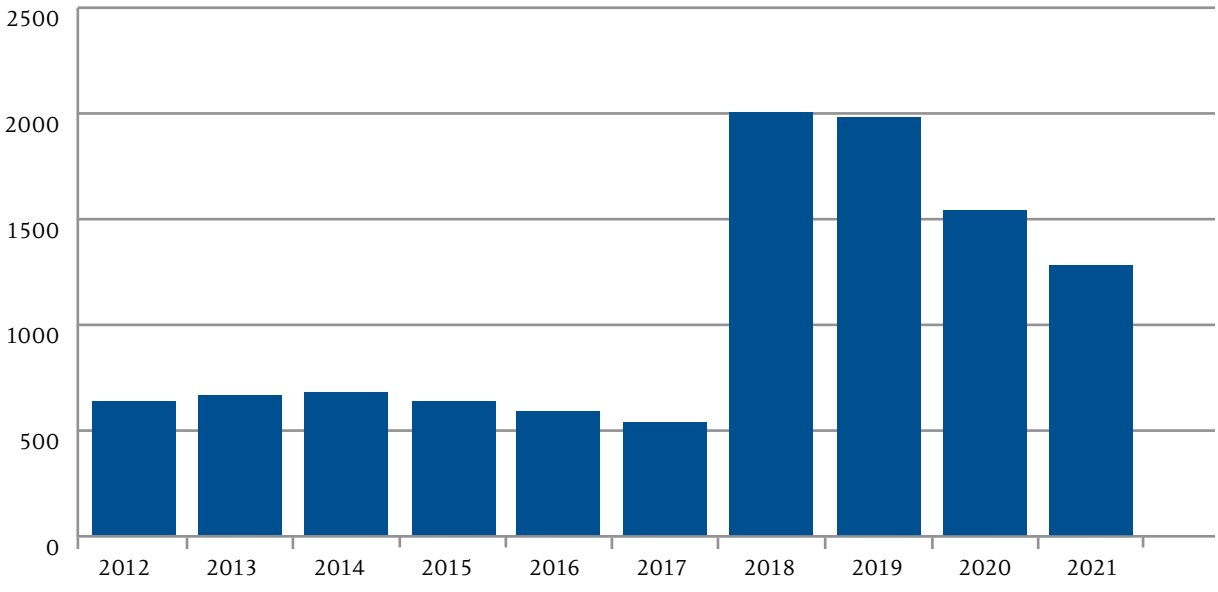


Abbildung 2: Anzahl der Anfragen pro Jahr

die Videoüberwachung auf das absolut erforderliche Mass beschränkt werden sollte. Trotz einer insgesamt konstruktiven Zusammenarbeit mit der verantwortlichen Stelle entschied sich diese schliesslich, die Vorgaben der DSS nicht umzusetzen. Nachdem die Frist der DSS zur Umsetzung ohne Rückmeldung verstrichen war, erliess die DSS eine Verfügung und ordnete die Einschränkung der Überwachungstätigkeit mittels Anweisung an. Diese Verfügung wurde von der verantwortlichen Stelle bei der Beschwerdekommission für Verwaltungsangelegenheiten (VBK) angefochten. Eine rechtskräftige Entscheidung steht noch aus.

Daneben wurde die DSS im Rahmen der Errichtung einer Videoüberwachung in einer anderen, neu entstandenen öffentlichen Freizeitanlage ebenfalls beratend beigezogen. Es stellten sich ähnliche Fragestellungen wie im oben erwähnten Fall. Unter Anwendung desselben Massstabs kam die DSS auch hier zum Schluss, dass die Überwachungstätigkeit einzugrenzen ist, denn der Schutz des privaten Freizeitverhaltens von Bürgerinnen und Bürgern ist sehr hoch bzw. höher zu werten als die mit der Videoüberwachung verfolgten Ziele des Betreibers der Freizeitanlage. Letztere können keine umfassende Beobachtung des Freizeitverhaltens rechtfertigen, weswegen diese Beobachtung auf das unbedingt erforderliche Mass einzuschränken ist. Im Gegensatz zum oben erwähnten Fall wurden in diesem Rahmen alle Vorgaben der DSS umgesetzt.

Neben weiteren Beratungen von öffentlichen Stellen, Unternehmen und Privatpersonen war die DSS auch im Berichtsjahr wieder häufig mit Videoüberwachungen im Rahmen von Nachbarschaftsstreitigkeiten konfrontiert. In mehreren Fällen konnte von den Mitarbeitenden der DSS ein Einvernehmen zwischen den Parteien und eine datenschutzkonforme Ausgestaltung der Videoüberwachung oder sogar ein Verzicht darauf erzielt werden. Insgesamt nahm die Beratung bezüglich Videoüberwachungen 2021 aber erneut viel Zeit und Ressourcen in Anspruch. Neben allgemeinen Beratungen über die Möglichkeit zulässiger Videoüberwachungen gab die DSS auch in zahlreichen Fällen konkrete Hinweise zur individuellen, technischen Ausgestaltung von Videokameras sowie zur Form und zum Inhalt der Piktogramme.

Auch die Nutzung von Fotos und insbesondere deren Veröffentlichung auf Internetseiten und in den Sozialen Medien war ein zentrales Thema im Berichtsjahr. Die grundlegende Frage war jeweils, was es zu berücksichtigen gilt, wenn Fotos von öffentlichen Anlässen erstellt werden und diese öffentlich gemacht werden sollen. Veranstaltern oder auch beteiligten Dritten, wie beispielsweise Gemeinden, wird regelmässig ein berechtigtes Interesse zuerkannt, wonach sie die Durchführung der Veranstaltungen dokumentieren können und hierfür auch Fotos erstellen dürfen. Auch für eine Veröffentlichung von Fotos in Zusammenhang mit der Veranstaltung und einer Information der Öffentlichkeit hierüber besteht grundsätzlich ein berechtigtes Interesse. Dieses kann jedoch grundsätzlich nur als Rechtsgrundlage dienen, wenn es sich um Fotos der Veranstaltung handelt und Personen, auch wenn sie erkennbar sind, lediglich als «Beiwerk» abgebildet sind. Auf jeden Fall ist an geeigneter Stelle über die Aufnahmen zu informieren und den Teilnehmenden zu ermöglichen, den Aufnahmebereich zu meiden, wenn sie das wünschen. Handelt es sich um «Porträtfotos», ist regelmässig eine Einwilligung einzuholen. Diffiziler wird die Beurteilung, wenn Kinder betroffen sind. Deren Schutz ist nochmals höher zu werten. Erschwerend kommt hinzu, dass je nach Alter eine Einwilligung der Erziehungsberechtigten eingeholt werden muss. Die DSS ist sich bewusst, dass es sich hier um Abgrenzungsfragen handelt, die Fingerspitzengefühl und Datenschutzsensibilität der Anwender und Verantwortlichen erfordert. Aus diesem Grund steht die DSS auch gerne nach wie vor beratend zur Seite.

2.3 Verbindliche interne Datenschutzvorschriften

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

Schon vor der DSGVO wurde das Konzept der BCR ausgearbeitet und laufend verfeinert. Aufgrund des Erfolges wurde es mit der DSGVO «verrechtlicht» und nochmals konkretisiert. BCR bieten den Unternehmen den Vorteil, dass es sich um keine starre Vorgabe von Verpflichtungen handelt, sondern um ein flexibles und adaptierbares Konstrukt, welches ständig weiterentwickelt werden kann und sich somit problemlos an neue Gegebenheiten anpassen lässt.

Die DSGVO sieht vor, dass es für Unternehmen bezüglich Fragen zu den BCR eine federführende Aufsichtsbehörde gibt, welche für die BCR und deren Genehmigungsverfahren die zentrale Ansprechpartnerin ist. Weiters wurden vom Europäischen Datenschutzausschuss (EDSA) Leitlinien ausgearbeitet, welche eine Anleitung für Antragsteller bieten und Inhalte vorgeben. Um sicherzustellen, dass die Vorgaben für BCR

von allen europäischen Datenschutzbehörden möglichst einheitlich angewendet werden, wurde mittlerweile auch eine elektronische Diskussionsplattform eingerichtet, und es werden regelmässige Treffen einberufen, an denen offene Diskussionspunkte von allen europäischen Behörden abschliessend behandelt werden. Die Diskussionen rund um die weiteren Entwicklungen nach dem «Schrems II»-Urteil führten im Berichtsjahr zudem dazu, dass eine grundlegende Überarbeitung der genannten Leitlinien in die Wege geleitet wurde.

Ein weiteres zentrales und aktuelles Thema ist der Wunsch nach einer Vereinfachung der BCR-Verfahren ohne qualitative Einbussen. Da BCR erst nach einer Stellungnahme des EDSA von der federführenden Aufsichtsbehörde genehmigt werden können, sind grundsätzlich alle europäischen Datenschutzbehörden von jedem BCR-Verfahren betroffen. Bei Vertragsdokumenten von regelmässig über 40 Seiten zuzüglich Zusatzdokumenten ist dies ein immenser Arbeitsaufwand für die Aufsichtsbehörden, den nur wenige Behörden wirklich bewältigen können. In der Folge bedeutet dies, dass zum Teil Zustimmungen von einzelnen Mitgliedstaaten für BCR erteilt werden, ohne dass diese überhaupt inhaltlich analysiert und geprüft wurden. Nach Hochrechnungen der niederländischen Aufsichtsbehörde wird sich diese Situation noch zusätzlich verschärfen, da ein BCR-Verfahrensstopp kurz nach Einführung der DSGVO zu einem Stau geführt hat. Nach Wiederaufnahme der BCR-Verfahren im Jahr 2019 wird nun erwartet, dass die nun anstehenden Finalisierungen zu einem weiteren, beträchtlichen Mehraufwand führen könnten. Es wird daher auch über mögliche Vereinfachungen des Verfahrens diskutiert. Ein Abschluss der Diskussion konnte im Berichtsjahr jedoch nicht erreicht werden.

Wie im letzten Tätigkeitsbericht bereits erwähnt, betreut die DSS seit 2019 als federführende Aufsichtsbehörde ein weltweit tätiges, liechtensteinisches Unternehmen bei der Ausarbeitung von BCR. Parallel zu der Ausarbeitung dieser BCR fand die oben erwähnte Überarbeitung der Leitlinien des EDSA statt. Da neue Elemente und Voraussetzungen darin auch in bereits genehmigte BCR noch übernommen werden müssen, war es dem Unternehmen wie auch der DSS ein Anliegen, diese Punkte schon im Erarbeitungsprozess zu berücksichtigen. Aufgrund der kooperativen und unkomplizierten Zusammenarbeit konnte dies problemlos bewerkstelligt wie auch verschiedene Unklarheiten geklärt werden. Eine offene Frage beschäftigte die DSS jedoch insbesondere. Um Unternehmen bei der Ausgestaltung von BCR einen möglichst grossen Gestaltungsspielraum einzuräumen, werden von den Behörden auch umfassende BCR akzeptiert, welche gewährleisten sollen, dass der europäische Datenschutz grundsätzlich auf alle Datenverarbeitungen in allen Niederlassungen angewandt wird. Ein zentrales Element der BCR ist deshalb die Beschreibung ihres Geltungsbereiches. Im Rahmen intensiv geführter Diskussionen zwischen den europäischen Aufsichtsbehörden einigte man sich schliesslich darauf, dass selbst bei einer abgrenzenden Umschreibung des Geltungsbereiches im Sinne von «alle Datenverarbeitungen zu allen Zwecken bezüglich aller Betroffenen» eine erläuternde Liste anzuführen ist, in der die Zwecke, Datenkategorien und betroffene Drittstaaten pro Transfer konkret aufzulisten sind. Die von der DSS als federführende Aufsichtsbehörde betreuten BCR konnten mit dieser Klärung einen finalen Schritt hin zur Fertigstellung nehmen. Der Abschluss des formellen Prozesses wird 2022 erwartet.

Zusätzlich zu den kurz vor dem Abschluss stehenden BCR ist im Berichtsjahr ein weiteres weltweit tätiges Unternehmen aus Liechtenstein auf die DSS zugekommen und hat Interesse an der Ausarbeitung von BCR bekundet.

2.4 Auswahl konkreter rechtlicher Fragen

3G in Unternehmen

Ab dem 15. September 2021 hat die Regierung den liechtensteinischen Unternehmen erlaubt, die Überprüfung des Vorliegens eines Covid-19-Zertifikats der Mitarbeitenden zur Festlegung angemessener Schutzmassnahmen im Unternehmen vorzunehmen. Da der Status einer betroffenen Person im Hinblick auf das Vorliegen eines «grünen» Zertifikats (geimpft, negativ getestet, genesen) als besonders schutzwürdiges Gesundheitsdatum nach Art. 9 DSGVO wie auch gesellschaftspolitisch sensible Information einzustufen ist, sind strenge datenschutzrechtliche Prinzipien zu beachten.

Als Rechtsgrundlage für die Verarbeitung dieser Daten dient zunächst Art. 6 Abs. 1 Bst. c i.V.m Art. 9 Abs. 2 Bst. b oder g DSGVO (Arbeitsrecht oder gesetzliche Grundlage aufgrund eines erheblichen öffentlichen Interesses). Die entsprechende nationale gesetzliche Grundlage findet sich neu in Art. 8 Abs. 4 und 4a Covid-19-Verordnung. Die allgemeine Fürsorgepflicht des Arbeitgebers aus dem Arbeitsrecht wäre im Prinzip ebenfalls geeignet, ist als ausreichende gesetzliche Grundlage für Covid-Massnahmen in Unternehmen jedoch umstritten.

Sodann ist das Prinzip der Datenminimierung einzuhalten. Die erwähnte Rechtsgrundlage erlaubt derzeit nur das Überprüfen des Vorliegens eines Zertifikats, nicht aber eine Überprüfung der genauen Art

des Zertifikats oder seiner Gültigkeitsdauer etc. Können vom Verantwortlichen keine triftigen Gründe geltend gemacht werden (z.B. bestimmte Art der Tätigkeit der Arbeitnehmenden im Gesundheitsbereich), so darf er keine weiteren Details von den Arbeitnehmenden abfragen. Genau so wenig darf er eine Kopie des Zertifikats oder des Impfausweises anfertigen und im Personaldossier ablegen. Sollte eine rein visuelle Kontrolle der Zertifikate für die Schutzmassnahmen im Unternehmen nicht ausreichen und das Führen einer Liste erforderlich sein, so ist auch hier äusserste Zurückhaltung geboten und nur so viel Information zu erfassen wie unbedingt nötig. Sowohl Datenschutzrecht als auch die Covid-19-Verordnung selbst erlauben keine weitere Verwendung der Daten zu anderen Zwecken. Und schliesslich sind die Daten sobald wie möglich wieder zu löschen.

Ebenfalls zu beachten sind die Informationspflichten. Die Covid-19-Verordnung selbst schreibt vor, dass ein Arbeitgeber die vorgesehene Überprüfung des Vorliegens eines Covid-19-Zertifikats sowie die daraus abgeleiteten Massnahmen zur Umsetzung eines angemessenen Schutzkonzepts schriftlich festhalten und seine Mitarbeitenden vorgängig dazu anhören muss. Werden die Daten in einer Liste o.ä. erfasst und gespeichert, so hat er darüber hinaus die datenschutzrechtlichen Informationspflichten aus Art. 13 DSGVO zu erfüllen und die Mitarbeitenden über die Eigenschaften dieser Datenverarbeitung zu informieren.

Gibt eine betroffene Person ihren genauen Status dem Arbeitgeber jedoch vollkommen freiwillig, ohne gefühlten Druck und unaufgefordert bekannt, so liegt eine gültige datenschutzrechtliche Einwilligung gemäss Art. 6 Abs. 1 Bst. a und Art. 7 DSGVO vor und die Information darf auch verarbeitet werden. Zu beachten ist hierbei dennoch, dass Einwilligungen im Beschäftigungskontext grundsätzlich immer heikel sind, da die Freiwilligkeit oftmals nicht gegeben ist. Ausserdem können sie jederzeit widerrufen werden. Nichtsdestotrotz erachtet die DSS es als legitimes Vorgehen, dass ein Arbeitgeber seinen Mitarbeitenden grundsätzlich die Möglichkeit anbietet, die Informationen freiwillig bekannt zu geben, um ein wiederkehrendes Überprüfen des Zertifikats zu vermeiden. Im Übrigen kann der Arbeitgeber seine Schutzmassnahmen jedoch nur auf den Status «Vorliegen eines grünen Zertifikats» oder «kein Vorliegen eines grünen Zertifikats» abstellen, da für eine weitere Differenzierung etwa nach «geimpft», «genesen» oder «getestet» derzeit die rechtliche Grundlage fehlt. Dies unterliegt jedoch dem Vorbehalt, dass von der Regierung oder dem Amt für Gesundheit keine andere Verlautbarung bzw. Anpassung der gesetzlichen Grundlage aus gesundheitspolizeilicher Sicht erfolgt.

Grundsätzlich empfiehlt die DSS allen Arbeitgebern die 3G-Regel nur dann anzuwenden, wenn dies tatsächlich für die Festlegung angemessener Schutzmassnahmen im Unternehmen erforderlich ist. Aus Gründen der Verhältnismässigkeit kann es durchaus auch angebracht sein, auf mildere Mittel (z.B. Abstandhalten, Split Teams, Home-Office) zurückzugreifen. Entscheidet man sich jedoch für die Einführung der 3G-Regel, so sollte sie möglichst datensparsam zum Einsatz kommen und beispielsweise nur mit einer visuellen Kontrolle der Zertifikate, ohne Erfassung in einer Liste durchgeführt werden. Ist jedoch eine Erfassung und Speicherung der sensiblen Daten unumgänglich, so sollten auf jeden Fall strenge Massnahmen zur Datensicherheit und Zugriffskontrolle vorgesehen werden. Ist ein Betriebsarzt vorhanden, könnte auch diesem die Überprüfung der Zertifikate übertragen werden, da er zusätzlich der ärztlichen Schweigepflicht unterliegt. Zu beachten ist ferner, dass eine Weitergabe oder -verwendung der Daten zu anderen Zwecken nicht erlaubt ist und sie sobald wie möglich wieder zu löschen sind.

Auskunftsrecht

Mehrere betroffene Personen als auch Verantwortliche stellten die Frage, ob im Rahmen der Auskunftserteilung nach Art. 15 DSGVO auch eine Information über technische und organisatorische Massnahmen (TOM) erteilt werden muss. Die Frage konnte von der DSS mit einem Nein beantwortet werden. Weder Art. 13 oder 14 DSGVO noch Art. 15 DSGVO begründen einen Rechtsanspruch auf Informationen zu TOM. Lediglich im Verarbeitungsverzeichnis gemäss Art. 30 DSGVO hat eine allgemeine Beschreibung der TOM zu erfolgen. Dieses Verzeichnis muss allerdings nicht gegenüber betroffenen Personen offengelegt werden. Ebenso sind TOM etwa in den Auftragsverarbeitungsvertrag aufzunehmen, aber auch hier gibt es keinen Anspruch betroffener Personen auf Einsicht.

Datenverarbeitung im Rahmen der Energiekataster

Gemäss Art. 35a Abs. 1 des Gesetzes über die Förderung der Energieeffizienz und der erneuerbaren Energien (Energieeffizienzgesetz; EEG) werden zur Sicherstellung einer nachhaltigen Energiestrategie und -planung über den Energie- und Wasserverbrauch auf Landes- und Gemeindeebene Energiekataster geführt. Gemäss Art. 35c Abs. 2 enthalten die Energiekataster kumulierte Energie- und Wasserverbrauchsdaten mit Angaben über die räumliche Lage (betroffenes Gebiet oder Lage von Objekten), die Objektart sowie den Umfang und die Art der verbrauchten Energie bzw. die verbrauchte Wassermenge.

Der Datenschutzbeauftragte der Gemeinden und eine Wasserversorgung wandten sich an die DSS mit der Frage, ob es datenschutzrechtlich zulässig sei, dass die Wasserversorgung eine Liste mit Ein-Personen-Objekten zur Verfügung gestellt bekäme, in welche sie den jeweiligen Wasserverbrauch für diese Objekte eintragen und in einem weiteren Schritt dann kumulieren sollte. Die Gemeinden und die Wasserversorgung erachteten diese Datenverarbeitung mittels der in der Liste vorhandenen Angaben zu den Ein-Personen-Objekten im Widerspruch zur Zweckbindung und der Datenminimierung.

Die DSS führte dazu aus, dass die Verarbeitung der Daten durch die Wasserversorgung mittels der Liste mit den Ein-Personen-Objekten mit den Datenschutzbestimmungen vereinbar und somit zulässig ist. Die Verarbeitung der personenbezogenen Daten mittels Liste ist erforderlich, damit die Wasserversorgung ihre gesetzliche Aufgabe erfüllen kann. Nur unter Zuhilfenahme dieser Liste kann sie den kumulierten Wasserverbrauch aller Ein-Personen-Objekte innerhalb einer Gemeinde und auf ein Jahr bezogen berechnen. Zusätzlich findet sich ein Verweis auf die Liste und die Zulässigkeit ihrer Verwendung in Art. 10 Abs. 3 der Verordnung vom 14. Juli 2020 über die Führung und Nutzung der Landes- und Gemeindeenergiekataster (Energiekatasterverordnung; EKV) selbst. Die DSS fügte hinzu, dass es im Verantwortungsbereich der Wasserversorgung liegt, dass sie die personenbezogenen Daten in der Liste ausschliesslich zu dem gesetzlich vorgesehenen Zweck verarbeitet, die Zuständigkeit auf ausgewählte Personen beschränkt und die Liste nach Ermittlung des Durchschnittswertes unverzüglich löscht

Verantwortlichkeit des Amtes für Justiz in Bezug auf personenbezogene Daten im Handelsregister

In Bezug auf personenbezogene Daten, die im Handelsregister eingetragen werden, stellte sich die Frage, ob das Amt für Justiz eine Verpflichtung hat, im Rahmen einer Eintragung in das Register die Verarbeitung von personenbezogenen Daten auf die Einhaltung der Datenschutzgrundsätze im Sinne des Art. 5 DSGVO zu prüfen. Konkret bedeutete dies die Frage, ob das Amt für Justiz im Zuge einer Eintragung ins Handelsregister alle eingereichten Unterlagen daraufhin überprüfen muss, ob in diesen ausschliesslich für den Zweck erforderliche Daten enthalten sind. Ebenso war fraglich, ob das Amt für Justiz eine Verpflichtung hat sicherzustellen, dass nur jene Daten vom Öffentlichkeitsprinzip erfasst werden, welche dem Zweck des Gesetzes dienen und zur Erfüllung der gesetzlichen Aufgabe erforderlich sind.

Die DSS bejahte grundsätzlich diese beiden Verpflichtungen. Wenn offensichtlich Daten in den eingereichten Unterlagen enthalten sind, die keinesfalls für die Eintragung erforderlich sind, sollte das Amt für Justiz diese Daten entsprechend den Grundsätzen der Zweckbindung und Datenminimierung nicht erheben bzw. in das Handelsregister eintragen.

Andererseits verlangt das Belegprinzip in Art. 961 Abs. 2 PGR, dass «In das Handelsregister nur Tatsachen eingetragen werden können, welche durch geeignete Urkunden als wahr belegt sind». Gemäss Art. 31 Abs. 2 der Verordnung über das Handelsregister (HRV) sind «bei der schriftlichen Anmeldung die Unterschriften zu beglaubigen». Art. 34 Abs. 1 ergänzt in Bezug auf die Firmaunterschrift, dass «eine Person, die zur Führung der Firmaunterschrift befugt ist, sie beim Amt für Justiz zu zeichnen oder in beglaubigter Form einzureichen hat». In Bezug auf diese eingereichten, geeigneten Urkunden kann nach Ansicht der DSS das Amt für Justiz davon ausgehen, dass in dem Falle, dass eine ausländische Urkunde zur Beglaubigung der Unterschrift einer natürlichen Person vorgelegt wird, diese Urkunde nur jene personenbezogenen Daten beinhaltet, die nach dem jeweiligen nationalen Recht für diese Beglaubigung erforderlich sind. Sollte sich trotz alledem herausstellen, dass die Rechtslage im Ausstellungsland der Urkunde die Aufnahme bestimmter personenbezogener Daten in eine Beglaubigung nicht gestattet, so wäre dies dort vor den zuständigen Behörden geltend zu machen.

«Streamen» bei standesamtlicher Hochzeit

Das Zivilstandsamt wandte sich mit der Frage an die DSS, ob es zulässig ist, dass ein Brautpaar ihre Vermählung am Zivilstandsamt «streame» und die Gäste der Zeremonie via Zoom folgen könnten. Im Prinzip fällt das Filmen / Streamen an Hochzeiten unter die sogenannte Haushaltsausnahme der DSGVO: Solange die Datenverarbeitung (Filmen / Streamen) ausschliesslich zur Ausübung persönlicher oder familiärer Tätigkeiten geschieht und nicht einem unbestimmten Personenkreis zugänglich gemacht wird, z.B. auf YouTube oder in einem Hochzeits-Blog ohne Login veröffentlicht wird, ist die DSGVO nicht anwendbar. Wird hingegen beabsichtigt, die Aufnahmen auf einem öffentlich zugänglichen Blog, Webseite oder sozialen Medien ohne Einschränkung auf einen definierten Familien- und Freundeskreis zu veröffentlichen, sind die Vorgaben der DSGVO zu berücksichtigen. In diesem Fall ist vorab von allen Personen, die von der Aufnahme direkt erfasst werden, einschliesslich von Mitarbeitenden des Zivilstandsamtes oder anderen aussenstehenden Drittpersonen, das Einverständnis gemäss Art. 7

DSGVO einzuholen. Andernfalls ist darauf zu achten, dass sie nicht von der Kamera erfasst werden.

Bekanntgabe von personenbezogenen Daten durch das Amt für Strassenverkehr

Von Seiten der Medien gelangte eine Anfrage an die DSS zur Frage, ob das Amt für Strassenverkehr auf Gesuch eines Tankstellenbetreibers personenbezogene Daten eines Fahrzeughalters herausgeben darf. Tankstellenbetreiber seien mitunter mit der Situation konfrontiert, dass Fahrzeughalter ihre Fahrzeuge an einer Tankstelle betankten, dann aber die Tankstelle verliessen, ohne die Rechnung zu bezahlen. Der Tankstellenbetreiber würde auf den Kosten der vorgenommenen Tankfüllung eines solchen Fahrzeughalters sitzen bleiben, wenn er den Fahrzeughalter nicht ausfindig machen und auf diese Weise den offenen Betrag einfordern könnte. Tankstellen sind heute meist mit einer Videoüberwachungsanlage ausgestattet. Bei Nichtbegleichung der Rechnung durch einen Fahrzeughalter kann der Tankstellenbetreiber auf die Videoaufzeichnungen zurückgreifen, um das Kennzeichen des Fahrzeugs festzustellen. Um die Personalien des Fahrzeughalters zu eruieren, gelangen die Tankstellenbetreiber in der Folge des Öfteren an das Amt für Strassenverkehr mit dem Gesuch, die Personalien des Fahrzeughalters zu erhalten. Ob eine entsprechende Herausgabe der Personalien eines Fahrzeughalters durch das Amt für Strassenverkehr in solch einem Fall gerechtfertigt sei, sollte nun von der DSS beantwortet werden.

Aus datenschutzrechtlicher Sicht war hierzu festzuhalten, dass es sich bei Personendaten eines Fahrzeughalters um personenbezogene Daten entsprechend Art. 4 Ziff. 1 DSGVO handelt, für welche die DSGVO und massgebende spezialgesetzliche Datenschutzbestimmungen anwendbar sind. Das Amt für Strassenverkehr muss damit über einen Rechtfertigungsgrund gemäss Art. 6 Abs. 1 DSGVO für die Verarbeitung der personenbezogenen Daten, hier die Offenlegung durch Weiterleitung an Dritte (Tankstellenbetreiber), verfügen. Das Amt für Strassenverkehr stützt sich hierbei auf Art. 99b Abs. 4 des Strassenverkehrsgesetzes (SVG). Dieser Artikel legt fest, dass das Amt «einer Person, die ein zureichendes Interesse glaubhaft machen kann, die Namen von Fahrzeughaltern und ihre Versicherer bekannt geben muss.»

Ein Tankstellenbetreiber, dessen Rechnung durch einen Fahrzeughalter nach Betankung nicht bezahlt wird, hat ein berechtigtes Interesse am Erhalt des Namens des Fahrzeughalters, um die nicht bezahlte Rechnung für die Tankbefüllung eintreiben zu können. Das berechtigte Interesse des Tankstellenbetreibers steht im gegebenen Kontext über den schutzwürdigen Interessen des Fahrzeughalters. Gemäss Art. 99b Abs. 4 SVG muss der Tankstellenbetreiber sein berechtigtes Interesse gegenüber dem Amt für Strassenverkehr jedoch glaubhaft machen. Dies geschieht durch Vorlage beweisender Mittel (insbesondere Videoaufzeichnung). Auf dieser Grundlage ist die Herausgabe der Personalien eines Fahrzeughalters an den Tankstellenbetreiber zur Einbringlichmachung seiner offenen Forderung aus der bisher nicht beglichenen Tankbefüllung erlaubt.

2.5 Auswahl konkreter technischer Fragen

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

Ist ein datenschutzkonformer Einsatz von Cloud Services generell möglich?

Die DSGVO als auch das DSG sind technikneutral formuliert und verbieten somit den Einsatz von Cloud Services nicht grundsätzlich, sondern stellen vielmehr allgemeine Regeln auf, die es auch bei der Nutzung von Cloud Services zu beachten gilt. Der Begriff der Cloud ist sehr weit gefasst und kann verschiedenste Ausprägungen vorweisen («Infrastructure as a Service» (IaaS), «Platform as a Service» (PaaS), «Software as a Service» (SaaS) etc.). Des Weiteren existieren diverse Modelle («Public», «Private», «Hybrid» etc.). Darüber hinaus lassen sich viele dieser Systeme in ihren Einstellungen und ihrer Architektur (z.B. Serverstandorte) individuell konfigurieren. Und schliesslich offerieren die Anbieter unterschiedlichste Lizenzmodelle und Service-Verträge. Deshalb ist die konkrete Einzelfallbetrachtung jeder individuell gewählten Lösung unabdingbar, um eine datenschutzrechtliche Beurteilung durchführen zu können. Die wichtigsten datenschutzrechtlichen Fragen bzw. Anforderungen hinsichtlich Cloud Services können in der Regel aber auf die folgenden fünf Punkte reduziert werden: Einhaltung datenschutzrechtlicher Grundsätze (Art. 5 DSGVO), Auftragsverarbeitungsvertrag (Art. 28 DSGVO), Einsatz von geeigneten technischen und organisatorischen Massnahmen (Art. 32 DSGVO), Datenschutz-Folgenabschätzung (Art. 35 DSGVO) sowie Einhaltung der Regelungen zum internationalen Datentransfer (Art. 44 ff. DSGVO). Details zu den einzelnen Punkten sind auf der Internetseite der DSS aufgeführt.

Welche Bestimmungen der DSGVO sind insbesondere für Techniker von Relevanz?

Aufgrund der zahlreichen und oft umfangreichen Artikel der DSGVO stellen sich Techniker bzw. IT-Verantwortliche oftmals die Frage, welches nun die Kern-

elemente innerhalb der DSGVO sind, die es aus technischer Sicht besonders zu beachten gilt. Vor diesem Hintergrund hat die DSS einen Spickzettel bzw. «Cheat-Sheet» zur DSGVO für die Praxis / Technik erarbeitet und auf ihrer Internetseite veröffentlicht. Um den Spickzettel möglichst kompakt und übersichtlich zu halten, erschien eine Reduzierung auf Kernaussagen und Grundsätze der DSGVO sinnvoll. In den Endnoten finden sich aber die entsprechenden Verweise, sodass bestimmte (technische) Massnahmen oder Vorgaben rasch der konkreten rechtlichen Bestimmung in der DSGVO zugeordnet werden können.

Welche (technischen) Aspekte sind besonders im Zusammenhang mit dem datenschutzkonformen Betrieb einer Internetseite zu beachten?

An die DSS gelangen immer wieder verschiedenste Fragen im Zusammenhang mit der datenschutzkonformen Erstellung bzw. Betrieb einer Internetseite. Eine der grundlegendsten Anforderung ist die Informationspflicht als Betreiber einer Internetseite (Datenschutzerklärung; Information der betroffenen Personen gemäss Art. 13 DSGVO). Selbst bei einer einfachen und kompakten Internetseite werden in der Regel personenbezogene Daten (z.B. IP-Adresse) verarbeitet. Aus diesem Grund ist selbst in diesem Fall eine Datenschutzerklärung notwendig. Selbstredend wird diese vom Umfang her kürzer ausfallen als bei einem Betreiber einer Internetseite, wo eine umfassende Verarbeitung personenbezogener Daten erfolgt. Dennoch gilt es die formalen Anforderungen an eine Datenschutzerklärung zu beachten. Wie die DSS in der Vergangenheit feststellen musste, werden insbesondere Datenschutzerklärungen von verschiedenen Quellen «zusammengestückelt» und nicht auf die individuellen Anforderungen der eigenen Internetseite angepasst. Somit besteht das Risiko für den Betreiber, dass er sich unnötigerweise potentiellen Beschwerden Dritter aussetzt. Ein weiterer wichtiger Aspekt betrifft die Übermittlung personenbezogener Daten an Drittländer ausserhalb des EU / EWR-Raumes oder an internationale Organisationen. Insbesondere nach dem «Schrems II»-Urteil des EuGH vom 20. Juli 2020 im Zusammenhang mit US-Anbietern von Webservices gilt es besondere Vorsicht bei der Evaluierung bzw. Implementierung walten zu lassen.

Kann ein Webseitenbetreiber mit der IP-Adressen-Anonymisierung von Webseitenbesuchern verhindern, dass die DSGVO Anwendung findet?

An die DSS gelangen immer wieder ähnliche Fragestellungen im Zusammenhang mit dem Betreiben einer Internetseite. Eine davon lautet, ob beim blossen Besuch einer Internetseite bereits personenbezogene Daten verarbeitet werden. Um diese Frage beantworten zu können, ist es hilfreich, den technischen Ablauf, der sich beim Besuch einer Internetseite abspielt, näher zu betrachten. Grundsätzlich wird vom Endgerät (Client) des Webseitenbesuchers eine Verbindung zum Webserver aufgebaut und in der Folge werden via «http» bzw. «https» Nachrichten ausgetauscht. Unter anderem wird dem Webserver auch die IP-Adresse des Clients mitgeteilt. Dass eine IP-Adresse in der Regel als personenbezogenes Datum zu qualifizieren ist, wurde bereits von verschiedenen Gerichten bestätigt. Um dies zu umgehen, wird häufig argumentiert, dass mit der Anonymisierung der IP-Adresse des Clients der Anwendungsbereich der DSGVO ausgeschlossen wird. Diese Annahme ist aus mehreren Gründen kritisch zu hinterfragen. Grundsätzlich gilt es, den exakten Anonymisierungsprozess zu analysieren und auf etwaige Schwachstellen zu überprüfen. Doch selbst wenn die IP-Adresse tatsächlich anonymisiert wird, können seitens Webserver weitere (personenbezogene) Daten vom Client angefragt und verarbeitet werden. Als Beispiel können das Browser- oder auch Canvas-Fingerprinting als Methode zur Informationsgewinnung bzw. konkreter, als Methode zur Identifizierung des Clients genannt werden. Anhand verschiedener Browser-Einstellungsmerkmale, installierter Plug-Ins und gegebenenfalls weiterer Parameter ist mit sehr hoher Wahrscheinlichkeit eine Identifizierung einzelner Besucher möglich. Forschende der Princeton University haben auf diese Methoden bereits 2014 in ihrer Arbeit hingewiesen. Die zu Beginn gestellte Frage kann somit nicht generell beantwortet werden. Es kommt darauf an, welche Daten konkret vom Betreiber der Webseite verarbeitet werden. Des Weiteren ist zu beachten, dass gemäss Art. 32 DSGVO die Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen ist. Im Sinne der Anforderung der Datensicherheit sind unter anderem entsprechende Protokolldaten beim Webseitenbesuch für einen beschränkten Zeitraum zu speichern. In diesem Zusammenhang ist die zweckmässige Speicherung von IP-Adressen aus Datenschutzsicht durchaus als angemessen zu betrachten.

«Die DSS stellt fest, dass sich aufgrund der Übernahme von Fachbegriffen aus der Schweizer Datenschutzgesetzgebung immer wieder Unstimmigkeiten im Vergleich zur Terminologie der DSGVO ergeben.»

3. Stellungnahmen zu Vorlagen und Erlassen

3.1 Stellungnahme zur Totalrevision des Gesetzes über die Reduktion der CO2-Emissionen (CO2-Gesetz)

Aus dem Vernehmlassungsbericht geht hervor, dass die Regierung mit dieser Gesetzesvorlage der völkerrechtlichen Verpflichtung aus Art. 1 Abs. 1 der am 14. April 2011 in Kraft getretenen Vereinbarung zwischen Liechtenstein und der Schweiz vom 29. Januar 2010 betreffend die Umweltabgaben im Fürstentum Liechtenstein nachkommt. Danach übernimmt Liechtenstein die Vorschriften der schweizerischen Bundesgesetzgebung über die Umweltabgaben in sein Landesrecht.

In Bezug auf die Artikel 30 und 32 der Vorlage, welche den Datenschutz betreffen, konnte die DSS feststellen, dass sich aufgrund der Übernahme von Fachbegriffen aus der Schweizer Datenschutzgesetzgebung einige Unstimmigkeiten im Vergleich zur Terminologie der DSGVO ergaben, die es zu korrigieren galt. In der Vorlage wurde etwa ausgeführt, dass das Amt für Umwelt in Art. 30 Abs. 2 «zur Bearbeitung und zur elektronischen Speicherung «personenbezogener Daten» im Sinne der Datenschutzgesetzgebung autorisiert wird» und «Personendaten, einschliesslich besonders schützenswerter Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen bearbeiten kann». Diese Aufzählung von personenbezogenen Daten unterschiedlicher Kategorien in einem Artikel weicht von der Terminologie der DSGVO ab, da die genannten Daten hier in zwei unterschiedlichen Artikeln geregelt werden und unterschiedlichen Kriterien für die Verarbeitung unterliegen. Art. 10 DSGVO regelt konkret «die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmassregeln». Art. 9 DSGVO hingegen regelt «die Verarbeitung besonderer Kategorien personenbezogener Daten».

Eine weitere Unklarheit folgte aus Art. 32 der Vorlage. Gemäss dessen Abs. 3 kann die Regierung mit Verordnung festlegen, welche Kategorien personenbezogener Daten verarbeitet werden dürfen und wie lange die Daten aufzubewahren sind. Gleichzeitig überträgt Art. 70 Abs. 3 des Schweizer Bundesgesetzes über die Verminderung von Treibhausgasemissionen (CO2-Gesetz) dem Bundesrat die Kompetenz, festzulegen, welche Kategorien von Personendaten bearbeitet werden dürfen und wie lange die Daten aufzubewahren sind. Nachdem gemäss Art. 30 der Gesetzesvorlage die in der Schweiz für den Vollzug der CO2-Gesetzgebung zuständigen Bundesbehörden dieses liechtensteinische Gesetz vollziehen, stellt sich die Frage, ob Art. 32 Abs. 3 verpflichtend eine Übernahme der Schweizer Festlegung der Kategorien der personenbezogenen Daten sowie der Speicherdauer bedeutet oder ob Liechtenstein hier einen Spielraum hat. Die DSS regte folglich an, dieses Zusammenspiel zumindest in den Materialien transparent zu erläutern.

3.2 Stellungnahme zur Schaffung eines Gesetzes über die Familienhilfe Liechtenstein (FHLG)

Die DSS regte an, einen Artikel in das Gesetz aufzunehmen, der die Rechtmässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten gemäss Art. 9 Abs. 2 DSGVO gewährleistet. Grundsätzlich ist mit Art. 9 Abs. 2 Bst. h DSGVO dafür eine datenschutzrechtliche Grundlage gegeben, allerdings verlangt diese Verordnungsbestimmung, dass entweder eine explizite Gesetzesbestimmung im Unionsrecht oder dem Recht eines Mitgliedstaats diese Datenverarbeitung zu einem konkreten Zweck erlaubt oder ein Vertrag mit einem Angehörigen eines Gesundheitsberufs vorliegt. Zudem muss gemäss Art. 9 Abs. 3 DSGVO gewährleistet werden, dass die Verarbeitung nach Art. 9 Abs. 2 Bst. h DSGVO durch Personal erfolgt, das einer besonderen Geheimhaltungspflicht unterliegt. Auch dieses Kriterium sollte in das revidierte Gesetz Eingang finden.

3.3 Weitere Stellungnahmen

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

- Abänderung des Bankengesetzes (BankG) sowie die Abänderung weiterer Gesetze;
- Abänderung des Markenschutzgesetzes (Umsetzung der Richtlinie (EU) 2015/2436 über die Marken);
- Erlass eines Gesetzes über die Nachhaltigkeit im Finanzdienstleistungssektor zur Durchführung der Verordnung (EU) 2019/2088 über nachhaltigkeitsbezogene Offenlegungspflichten im Finanzdienstleistungssektor und der Verordnung (EU) 2020/852 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088 über nachhaltigkeitsbezogene Offenlegungspflichten

im Finanzdienstleistungssektor (EWR-Durchführungsgesetz über die Nachhaltigkeit im Finanzdienstleistungssektor; EWR-NHFDG) sowie Erlass eines Gesetzes über die Abänderung des Finanzmarktaufsichtsgesetzes (FMAG);
- Änderung des EWR-Wertpapierprospekt-Durchführungsgesetzes, des Bankengesetzes (BankG), des Vermögensverwaltungsgesetzes (VVG) und des EWR- Verbriefungs-Durchführungsgesetzes (Massnahmenpaket für die Erholung der Kapitalmärkte).

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

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

4. Interne Organisation

Die DSS ist die nationale Datenschutz-Aufsichtsbehörde im Sinne des Art. 51 DSGVO sowie 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 sowie einzelnen Bestimmungen in Spezialgesetzen.

4.1 Personal allgemein

Die DSS konnte die an sie gestellten Anforderungen im Berichtsjahr mit dem bestehenden Personal von 700 Stellenprozenten sehr gut erfüllen. Die bereits in den Vorjahren praktizierte intensive Zusammenarbeit zwischen Technik und Recht war auch im Berichtsjahr unabdingbar für die meisten Tätigkeiten. Insbesondere die Frage nach der Zulässigkeit von Webanalyse-Tools etc. war fast täglich präsent und der Datentransfer in ein unsicheres Drittland verlangte nach vertieftem technischem Verständnis.

Zudem konnte die DSS im ersten Halbjahr einen Praktikanten mit rechtswissenschaftlicher Ausbildung mit einem Pensum von 80 Stellenprozenten beschäftigen. 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 im Schengen-Raum sehen vor, dass diese alle vier Jahre einer datenschutzrechtlichen Kontrolle unterzogen werden müssen. Bis 2019 konnte eine liechtensteinische Beteiligung an diesen datenschutzrechtlichen Kontrollen auf Grund begrenzter personeller Ressourcen der DSS nicht oder nur in sehr eingeschränktem Rahmen vorgenommen werden. Die vom Landtag 2019 bewilligte zusätzliche Stelle erlaubte es der DSS aber, ihren Verpflichtungen im Rahmen der Teilnahme Liechtensteins am Schengen-Raum auch 2021 wieder vollumfänglich nachzukommen.

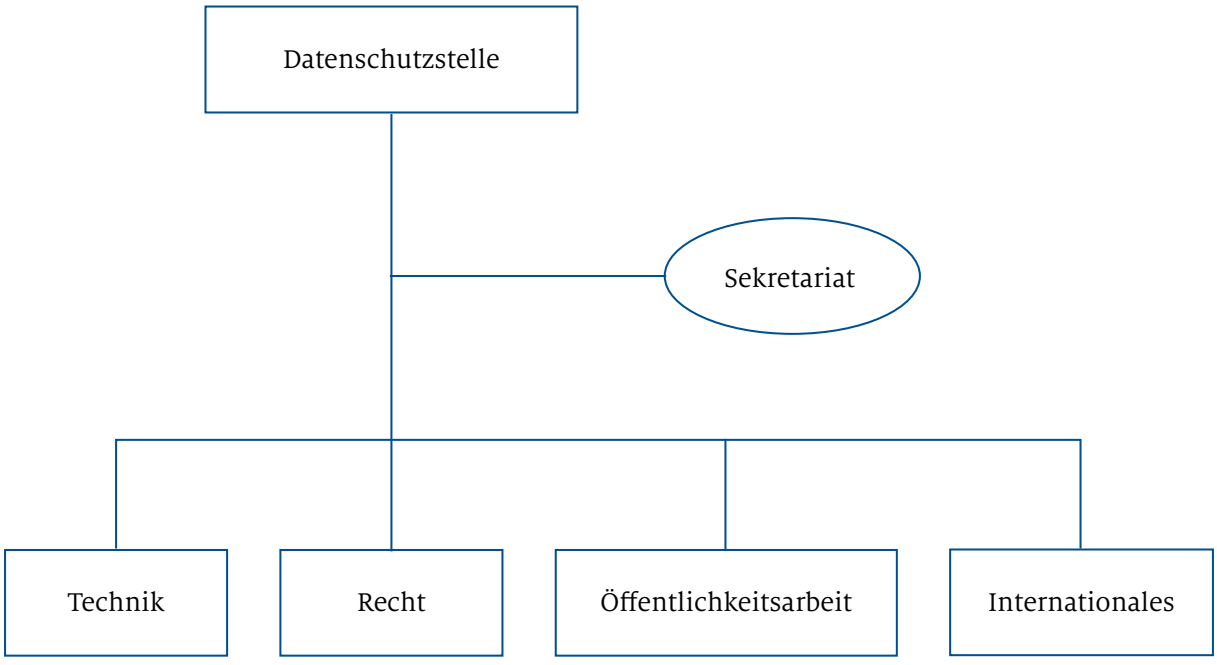


Abbildung 3: Organigramm Datenschutzstelle

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

5. Aufsicht, Beschwerden und Meldungen von Datenschutzverletzungen

5.1 Aufsicht

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

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

Aufgrund der schwierigen Lage für viele Unternehmen angesichts der Covid-19-Pandemie entschied die DSS, im Berichtsjahr von amtswegigen Untersuchungen bei Unternehmen abzusehen, ausser in jenen Fällen, in denen die DSS Informationen von Privatpersonen oder anderen Behörden in Bezug auf einen vermeintlichen Datenschutzverstoss erhielt, die Informanten aber keine formelle Beschwerde im Sinne des Art. 77 DSGVO einbringen wollten. Hingegen führte die DSS in Zusammenhang mit Schengen eine amtswegige Datenschutzüberprüfung bei der Landespolizei durch und begleitete die Schengen-Evaluationen von Liechtenstein und Malta. Ausserdem nahm die DSS eine weitere amtswegige Datenschutzüberprüfung im Bereich des Zentralen Personenregisters (ZPR) bzw. dessen Nachfolgeprodukt, den Zentralen Stammdaten (ZSD), vor.

5.1.1 Amtswegige Überprüfungen in Zusammenhang mit Schengen

Interne Prüfung des Schengener Informationssystems der zweiten Generation (SIS II)

Mit dieser Prüfung wurde dem geltenden Rechtsrahmen entsprochen, wonach unter anderem die Datenverarbeitungsvorgänge betreffend das Schengener Informationssystem der zweiten Generation (SIS II) in regelmässigen Abständen durch die DSS nach internationalen Prüfstandards zu überprüfen sind.

Der nationale Teil des Schengener Informationssystems der zweiten Generation (SIS II) wird durch die Landespolizei (LP) betrieben und enthält zahlreiche Informationen zur Identifizierung natürlicher Personen oder Sachen sowie zu den zu ergreifenden Massnahmen. Die Datenschutzüberprüfung wurde als sogenannte Protokollprüfung bzw. Dokumentenprüfung durchgeführt, sprich eine Prüfung vor Ort fand nicht statt. Mitgliedstaaten, die – wie Liechtenstein – keine nationalen Kopien des SIS II verwenden, haben sicherzustellen, dass unter anderem jeder Zugriff auf personenbezogene Daten im System protokolliert wird. Anhand der Protokolldaten kann sowohl die Rechtmässigkeit der Abfrage überprüft und eine entsprechende Selbstkontrolle durchgeführt werden als auch das einwandfreie Funktionieren des SIS II sowie die Datenintegrität und Datensicherheit gewährleistet werden. Augenmerk bei der Analyse der Zugriffsprotokolle wurde gegenständlich unter anderem auf die Direktabfragen auf das Produktivsystem des SIS II durch das Amt für Strassenverkehr (ASV) gelegt. Die Abfragemöglichkeit für das ASV im SIS II besteht seit Herbst 2019. So kann das ASV zum alleinigen Zweck der Überprüfung, ob das ihnen zur Zulassung vorgeführte Fahrzeug gestohlen, unterschlagen oder sonst abhandengekommen ist und ob die Fahrzeugpapiere und Motorfahrzeug-Kennzeichen für ungültig erklärt worden sind, im SIS II abfragen. Die Prüfung der Zugriffe durch das ASV ergab jedoch keine Unregelmässigkeiten oder Beanstandungen. Ein weiterer Fokus der Datenschutzüberprüfung lag auf dem Zugriff durch externe Dienstleister, die auf den Systemen des SIS II bei der LP über erweiterte Benutzerrechte verfügen. Dabei sind durch die LP insbesondere die Anforderungen an die Sicherheit der Datenverarbeitung gemäss Art. 63 DSG zu berücksichtigen. Dieser Teil der Datenschutzüberprüfung konnte im Berichtsjahr noch nicht vollständig abgeschlossen werden.

Schengen-Evaluation Liechtenstein

Da die letzte Schengen-Evaluation Liechtensteins im Jahr 2015 stattgefunden hatte, stand im Berichtsjahr die nächste Kontrolle an. Bedingt durch die Co-

vid-19-Beschränkungen wurde die Vor-Ort-Kontrolle zunächst verschoben und schliesslich digital durchgeführt. Im Rahmen der Überprüfungen durch das Expertenteam wurden zunächst die Empfehlungen vorheriger Evaluationen berücksichtigt wie auch die von der DSS selbst durchgeführten Kontrollen und ihre diesbezüglichen Empfehlungen den Experten zur Verfügung gestellt. Während der Kontrolle selbst erhielten die Experten ausführliche und transparente Informationen über nationale Gesetzesumsetzungen, Abläufe, durchgeführte Kontrollen, Statistiken wie auch Anfragen, Beschwerden und Zugriffsrechte. Im Zuge der Evaluation wurden schliesslich von der Expertengruppe sechzehn Empfehlungen ausgesprochen. In Bezug auf datenschutzrechtliche Aspekte ist zu erwähnen, dass gefordert wurde, die DSS mit effektiven Abhilfemassnahmen nach Art. 47 Abs. 2 LED (Polizei-Richtlinie (EU) 2016 / 680) auszustatten. Die Kritik bezog sich konkret darauf, dass auf Grundlage der aktuellen Rechtslage im nationalen DSG die DSS bei datenschutzrechtlichen Verfehlungen, welche unter die LED fallen, den Verantwortlichen lediglich über den Verstoss «informieren» kann, aber keine Verwarnungen aussprechen oder Anordnungen treffen darf, wie dies etwa im Rahmen der Aufsicht unter der DSGVO zulässig ist.

Schengen-Evaluation Malta

Für die datenschutzrechtliche Evaluation der diversen EU-Informationssysteme wird jeweils ein Expertenteam bestehend aus Mitarbeitenden der EU-Kommission wie auch EWR-Aufsichtsbehörden zusammengestellt, welches eine Vor-Ort-Kontrolle durchführt. Im Rahmen der regelmässigen Schengen-Evaluationen (Schengen-Acquis) entsandte auch die DSS selbst einen IT-Experten nach Malta, um dort die Einhaltung geltender Datenschutzbestimmungen durch die Informationssysteme zu überprüfen. Unter der Leitung der Generaldirektion Migration und Inneres (DG Home) der EU-Kommission führte eine Expertengruppe, bestehend aus Juristen als auch IT-Experten, während einer Woche im November vor Ort Begehungen, Interviews mit den maltesischen Behörden und deren IT-Dienstleistern sowie Dokumentenprüfungen durch. Gegenstand der Untersuchungen waren Datenverarbeitungsvorgänge im Zusammenhang mit dem Schengener Informationssystem der zweiten Generation (SIS II) sowie des Visa Informationssystems (VIS). Vor der eigentlichen Vor-Ort-Inspektion beantworteten die maltesischen Behörden unter anderem schon einen umfangreichen Fragebogen, so dass sich die Experten vorab ein gutes Verständnis über die Ausgangslage verschaffen konnten. Die maltesische Datenschutzbehörde (IDPC) stellte das Arbeitsprogramm für die Woche zusammen und begleitete die Expertengruppe während der ganzen Woche. Die Expertengruppe verfasste im Rahmen ihrer Arbeit vor Ort bereits den Entwurf des Evaluierungsberichts. Gemäss den Verfahrensschritten des Schengen-Evaluierungsmechanismus haben die maltesischen Behörden nach Zustellung des Entwurfs zwei Wochen Zeit, eine Stellungnahme dazu abzugeben. Am Ende der Verfahrensschritte ist die Berichterstattung der Behörden über die Umsetzung des im Bericht vorgegebenen Aktionsplans vorgesehen – sofern Mängel hinsichtlich der Datenverarbeitungsvorgänge festgestellt worden sind.

5.1.2 Amtswegige Überprüfung: ZPR/ZSD

Eine weitere Datenschutzüberprüfung betraf das von der Landesverwaltung betriebene Zentrale Personenregister (ZPR) bzw. das Nachfolgeprodukt, die Zentralen Stammdaten (ZSD). Es wurde geprüft, ob die technische Umsetzung sowie die organisatorischen Abläufe im Zusammenhang mit der Protokollierung der Zugriffe datenschutzkonform ausgestaltet sind. Die Datenschutzüberprüfung wurde ebenfalls als sogenannte Dokumentenprüfung durchgeführt, sprich auch hier fand keine Prüfung vor Ort statt. Im Zusammenhang mit dem ZPR sind aktuell die Bestimmungen aus dem geltenden Gesetz über das Zentrale Personenregister (ZPRG) zu berücksichtigen. Für die gegenständliche Datenschutzüberprüfung wurde – wo sinnvoll und angemessen – bereits der Status quo der Revision zum ZPRG mitberücksichtigt. Zusammenfassend konnte bei der gegenständlichen Datenschutzüberprüfung festgestellt werden, dass die Verarbeitung der personenbezogenen Daten durch die verantwortliche Stelle im Zusammenhang mit dem ZSD im Kern datenschutzkonform erfolgt. Insgesamt ist die Haltung der verantwortlichen Stelle gegenüber dem Datenschutz und dem Schutz der Persönlichkeit und Privatsphäre der betroffenen Personen sowie gegenüber der Datensicherheit als positiv hervorzuheben. Ungeachtet dessen wurden in wenigen Punkten Mängel festgestellt, die adressiert und mit entsprechenden Massnahmen behoben werden müssen. Dies DSS wird die Landesverwaltung und die mit dem Betrieb der Systeme betrauten Stellen entsprechend bei der Lösungsfindung und Mängelbehebung unterstützen.

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 Erwä-

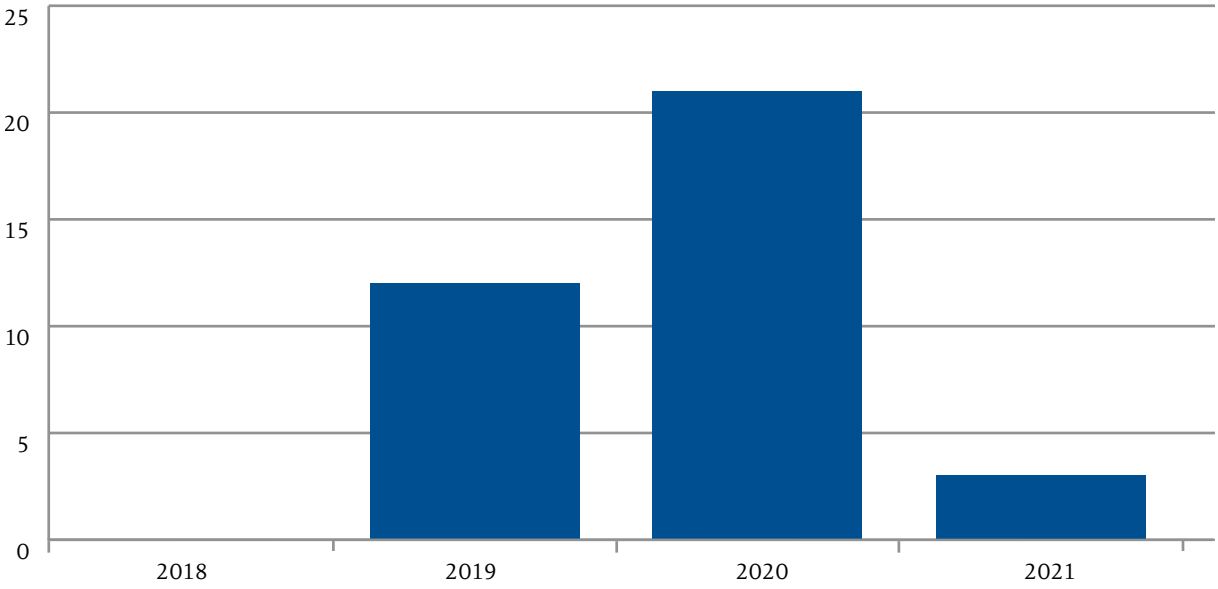


Abbildung 4: Anzahl der Datenschutzüberprüfungen pro Jahr

gungsgrund 141 der DSGVO empfohlen – auf ihrer Internetseite in der Rubrik «Services» ein elektronisches Beschwerdeformular an.

Im Berichtsjahr erhielt die DSS insgesamt 56 Beschwerden von Privatpersonen, die sich direkt an die DSS als für ein liechtensteinisches Unternehmen oder eine öffentliche Stelle zuständige Aufsichtsbehörde richteten. Die Beschwerdeführer haben zum überwiegenden Teil ihren Wohnsitz in Liechtenstein. Aber auch Personen aus dem EU/EWR-Raum, vor allem Deutschland und Österreich, brachten Beschwerden bei der DSS ein. Hinzu kam eine Person aus einem Drittstaat. Eine Beschwerde wurde von einem Bürger in Liechtenstein gegen ein Unternehmen in Deutschland eingebracht und von der DSS an die federführende Behörde in Deutschland weitergeleitet. Umgekehrt erhielt die DSS im Rahmen der Zusammenarbeit mit den anderen Aufsichtsbehörden im EU/EWR-Raum unter Art. 56 ff. DSGVO im Berichtsjahr zwei weitere Beschwerden von Personen aus einem anderen Mitgliedstaat, die sich jeweils gegen ein liechtensteinisches Unternehmen richteten.

Nicht eingerechnet in diese Zahl sind Anfragen von betroffenen Personen, bei denen sich herausstellte, dass die Beschwerde keine Verarbeitung von sie persönlich betreffenden personenbezogenen Daten zur Grundlage hatte. Damit lag die Anzahl der Beschwerden gemäss Art. 77 DSGVO bei der DSS knapp 8 % unter der Anzahl des Vorjahres.

Auch 2021 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 2021 keine verhängt. Damit ist die DSS im Vergleich zu den anderen europäischen Behörden eher die Ausnahme, denn die Geldbussen nehmen im EWR beständig zu und werden gerade in Fällen von beharrlichen und weitreichenden Datenschutzverletzungen oft als das einzige tatsächlich abschreckende Mittel gesehen.

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

troffenen Personen auszurichten ist. So muss eine 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 Beschwerde-Fall bildete eine Verfügung den Abschluss des Verfahrens. Stattdessen konnte in einigen Fällen mit der datenverarbeitenden Stelle eine (einvernehmliche) Lösung gefunden werden, die es erlaubte, die Rechte der Betroffenen zu gewährleisten. Mit diesem auch in Erwägungsgrund 131 der DSGVO empfohlenen Vorgehen konnten im Berichtsjahr zahlreiche langwierige und aufwändige Verfahren verhindert werden.

5.2.1 Ausgewählte Verfügungen der DSS im Berichtsjahr

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

Ein Beschwerdeführer machte geltend, dass von einem Verantwortlichen im Rahmen eines Gewinnspiels Art. 5 Abs. 1 Bst. c DSGVO, Art. 6 Abs. 1 Bst. a i.V.m. Art. 7 DSGVO ebenso wie Art. 13 DSGVO verletzt worden seien. Gemäss dem Talon bzw. der Internetseite des Unternehmens in Bezug auf den Wettbewerb könne man nur teilnehmen, wenn man «wie üblich» die Teilnahmebedingungen des Unternehmens akzeptiere. Zudem würden Daten für die Teilnahme erhoben, die über den Zweck des Gewinnspiels hinausgingen.

Die Frage der Verletzung des Grundsatzes der Datenminimierung gemäss Art. 5 Abs. 1 Bst. c DSGVO war von der DSS zu bejahen, da vom Verantwortlichen für die Durchführung des Gewinnspiels nicht erforderliche Daten wie Geburtsdatum, Geschlecht und Krankenversicherung erhoben wurden.

Ebenso war die Frage der Verletzung des Art. 6 Abs. 1 Bst. a i.V.m. Art. 7 DSGVO von der DSS zu bejahen. Entscheidend für eine rechtmässige Einwilligung ist, dass für den Wettbewerbsteilnehmer von vornherein klar, verständlich und nachvollziehbar ist, wozu er einwilligt. Erwägungsgrund 32 DSGVO spezifiziert ähnlich wie Art. 4 Ziff. 11 DSGVO, dass die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen sollte, mit der freiwillig, für den konkreten Fall, in informierter Weise unmissverständlich bekundet wird, dass die betroffene Person, bzw. aktuell der Wettbewerbsteilnehmer, mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Dies kann etwa in Form einer schriftlichen Erklärung erfolgen, die auch elektronisch ausgestaltet sein kann. Um am gegenständlichen Wettbewerb teilnehmen zu können, mussten Wettbewerbsteilnehmer ein Häkchen bei folgendem Satz setzen: «Ich nehme am Wettbewerb teil und akzeptiere die untenstehenden Teilnahmebedingungen». Aus diesem Satz kann nicht eindeutig abgeleitet werden, dass damit eine Einwilligung im datenschutzrechtlichen Sinn abgegeben wird. Kein einziges

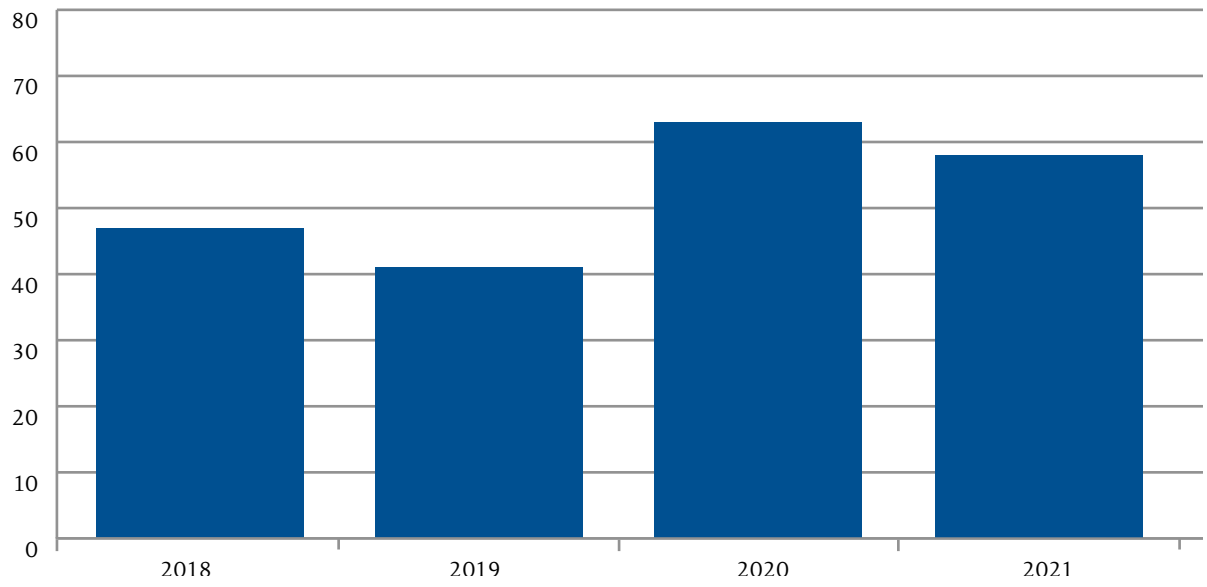


Abbildung 5: Anzahl der Beschwerden pro Jahr

Wort weist auf eine «Einwilligung» oder «Zustimmung» hin. Erst aus den in wesentlich kleinerer Schriftgrösse angeführten Teilnahmebedingungen kann abgeleitet werden, dass dieser Satz eine Einwilligung impliziert. Erst bei genauem Lesen der Teilnahmebedingungen erfährt der Wettbewerbsteilnehmer in Zeile 6, dass mit der Abwicklung des Gewinnspiels die Verwendung seiner Daten zu Werbezwecken und zur Kontaktaufnahme durch das Unternehmen selbst sowie ein weiteres Partnerunternehmen verbunden ist.

Artikel 6 Abs. 1 Bst. a DSGVO bestätigt, dass die Einwilligung der betroffenen Person für «einen oder mehrere bestimmte» Zwecke erteilt werden muss und dass eine betroffene Person in Bezug auf jeden dieser Zwecke eine Wahlmöglichkeit haben muss. Im vorliegenden Fall werden drei Zwecke vermengt: Abwicklung des Gewinnspiels sowie zu Werbezwecken und zur Kontaktaufnahme durch verschiedene Unternehmen.

Gemäss Art. 7 Abs. 3 DSGVO muss zudem die Möglichkeit des Widerrufs der Einwilligung gleich einfach wie die Erteilung der Einwilligung sein. Während das Unternehmen für die vermeintliche Einwilligung ein Kästchen zum Ankreuzen bereit stellte, fand sich in Bezug auf den Widerruf in den Teilnahmebedingungen lediglich der folgende Satz: «Diese Einverständniserklärung kann jederzeit und ohne Angaben von Gründen widerrufen werden». Zur Frage, wo und wie dies geschehen kann, finden sich keine direkten Informationen. Erst in der Datenschutzerklärung auf der Internetseite findet sich auf Seite 7 eine entsprechende E-Mail-Adresse.

Schliesslich war auch eine Verletzung der Informationspflicht gemäss Art. 13 DSGVO festzustellen. Auch wenn der vom Unternehmen ins Treffen geführte Mehrebenen-Ansatz vorliegend Anwendung finden kann, wäre dafür eine umfassende Information gemäss Art. 13 DSGVO auf der Internetseite des Unternehmens erforderlich, welche sämtliche Elemente enthält, die in Art. 13 DSGVO gefordert werden.

Die Wettbewerbsteilnehmer sind dabei unter anderem über die Art und Weise der Verarbeitung ihrer Daten, den konkreten Zweck sowie die Speicherdauer und Löschfrist entsprechend zu informieren, was allerdings gegenständlich nicht erfolgt ist, weshalb vorliegend der vom Unternehmen genannte Mehrebenen-Ansatz keine Relevanz erlangt.

Zwei Beschwerdeführer machten geltend, dass auf einer an liechtensteinischen Schulen genutzten Lernplattform die Sicherheit der von den Schülerinnen und Schülern angelegten Benutzerkonten nicht dem heutigen Stand der Technik entspräche, für den Kauf im Webshop keine Einwilligung gemäss Art. 8 DSGVO eingeholt würde und die Information gemäss Art. 13 DSGVO mangelhaft sei.

Die DSS bejahte alle drei Beschwerdepunkte. In Bezug auf die Information gemäss Art. 13 DSGVO war festzustellen, dass sich weder auf der Startseite noch auf Unterseiten ein expliziter Hinweis auf die Datenschutzerklärung findet. Es ist stattdessen dem Link «Impressum» zu folgen, um zur Datenschutzerklärung zu gelangen. Es ist zwar rechtlich möglich, beide Bereiche mit einem Link abzudecken, allerdings gemäss ständiger Rechtspraxis nur, wenn der Link dazu eindeutig auf beide Punkte hinweist. Etwa «Impressum & Datenschutz». Ebenso wenig liess sich aus den vorhandenen Informationen ableiten, wer für die Seite Verantwortlicher und wer Auftragsverarbeiter war bzw. wer für die Seite bzw. die Lernplattform als Ansprechperson bzw. Datenschutzbeauftragter fungierte.

In Bezug auf die Rechtsgrundlage besagte die Datenschutzerklärung, dass die Datenverarbeitung auf der Einwilligung beruhe. Dazu stellte die DSS fest, dass die Einholung einer Einwilligung innerhalb der Datenschutzerklärung nicht rechtskonform ist. Es war auch nicht klar, wofür konkret eine Einwilligung erforderlich ist und auf welchem Wege diese eingeholt wird.

In Bezug auf den Beschwerdepunkt der mangelhaften Einwilligung gemäss Art. 8 DSGVO beim Webshop gelangte die DSS zur Feststellung, dass Art. 8 DSGVO zum Zeitpunkt der Einbringung der Beschwerde klar verletzt war. Es handelte sich bei dem Webshop um ein i.S.d. Art. 8 Abs. 1 DSGVO bestehendes «Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird». Eine Testbestellung durch die DSS mit einer fiktiven E-Mail-Adresse zeigte, dass der Betreiber des Webshops keinerlei Massnahmen gesetzt hatte, um das Alter des Bestellers festzustellen oder die elterliche Einwilligung einzuholen, wodurch eine Verletzung von Art. 8 Abs. 1 und 2 DSGVO vorlag.

In Bezug auf die Sicherheit der Benutzerkonten stellte die DSS fest, dass technische Massnahmen zu ergreifen sind, sodass beispielsweise beim nächstmaligen Login nach der Anmeldung mit dem Initialpasswort eine Passwortänderung erzwungen wird. Im Lichte des Art. 32 DSGVO und des Erwägungsgrundes 38 DSGVO sowie der Tatsache, dass die Internetseite öffentlich zugänglich ist, erfolgte die Anweisung der DSS gemäss Art. 58 Abs. 2 Bst. d DSGVO, dass alle Benutzerkonten im Zusammenhang mit der Internetseite umgehend zu sperren waren, sodass eine Anmeldung mit den «alten» Initialpasswörtern oder Passwörtern nach dem alten Passwortschema verunmöglicht wurde.

Ein Beschwerdeführer brachte vor, dass der Verantwortliche im Rahmen der Beantwortung seines Auskunftsschreibens keine ausreichende Begründung gemäss Art. 12 Abs. 3 DSGVO vorbrachte und somit eine Verletzung von Art. 15 DSGVO gegeben war.
Die DSS gab der Beschwerde recht und begründete dies wie folgt: Art. 12 Abs. 3 DSGVO definiert zwei Voraussetzungen für die Fristverlängerung, nämlich die Komplexität und die Anzahl von Anträgen. Der Wortlaut «und» lässt den Schluss nahe, dass die beiden Voraussetzungen kumulativ vorliegen müssen. Allerdings ist dies in der Literatur nicht unumstritten und es findet sich auch die Meinung, dass eine der Voraussetzungen ausreicht. Nichtsdestotrotz ist die Bestimmung eng auszulegen, um Missbräuche und routinemässige Fristverlängerungen zu verhindern. Folglich genügt es nicht, den Gesetzeswortlaut als Begründung für die Fristverlängerung zu zitieren, sondern der Verantwortliche muss eine konkrete Begründung, die sich aus seiner individuellen und aktuellen Situation ergibt, anführen. Nur so kann überprüft werden, ob es sich um eine tatsächliche Erfüllung der in Art. 12 Abs. 3 DSGVO genannten Voraussetzungen handelt. Insbesondere bei der Anzahl der Anträge ist nachzuweisen, dass es sich im konkreten Fall um eine solche Anzahl handelt, die über das bei einem Verantwortlichen dieser Art und Grösse üblicherweise zu erwartende Mass deutlich hinausgeht. In Bezug auf die Komplexität ist festzustellen, dass es sich im vorliegenden Fall um keine komplexe Frage bzw. Abklärungen handelte, da bei ausreichenden organisatorischen und technischen Vorkehrungen eine solche Anfrage rasch hätte beantwortet werden können.

5.2.2 Urteile des Verwaltungsgerichtshofs (VGH)

2021 wurden fünf Beschwerden, die von der DSS mit Verfügung abgeschlossen wurden, nach Durchlaufen des Beschwerdeweges letztinstanzlich vom VGH entschieden.

Vier der letztinstanzlich entschiedenen Fälle (Fall 1: VGH 2021 / 031, VGH 2021 / 029, Fall 2: VGH 2021 / 032, VGH 2021 / 030, Fall 3: VGH 2020 / 050 und Fall 4: VGH 2020 / 051) ergingen zu Beschwerden, bei denen die Beschwerdeführer erster Instanz ihre Beschwerde gegen ein im Adresshandel tätiges Unternehmen in Liechtenstein gerichtet hatten. Allen vier Beschwerdefällen war gemeinsam, dass ihnen gleichartige Datenverarbeitungen zugrunde lagen und die Beschwerdeführer des Verfahrens erster Instanz eine mutmassliche Verletzung von Art. 5, 6 und 15 DSGVO rügten.

In zwei dieser beim Verwaltungsgerichtshof eingereichten Beschwerden (Fall 1 und Fall 2) gründete der VGH seine Entscheidungen massgeblich auf das Urteil des EFTA-Gerichtshofs vom 10. Dezember 2020 zur Frage der Anonymität und der Frage der Kostentragung der Verfahrens- und Parteikosten in einem Beschwerdeverfahren gemäss Art. 78 DSGVO. Die Beschwerden beim VGH wurden sowohl von der DSS als auch von der Beschwerdegegnerin erster Instanz beim Verwaltungsgerichtshof eingereicht und von diesem als verbundene Beschwerden behandelt. Was war geschehen? Eine Rekapitulation dieser Fälle im Überblick:

VGH-Urteil 2021 / 031, VGH 2021 / 029 (Fall 1) sowie VGH-Urteil 2021 / 032, VGH 2021 / 030 (Fall 2)
Die Beschwerdeführer sprachen sich bei Einreichung ihrer Beschwerde bei der DSS gegen eine Offenlegung ihrer Daten gegenüber der Beschwerdegegnerin erster Instanz aus. Die DSS hat im Verfahren erster Instanz die Möglichkeit der Anonymität der Beschwerdeführer nach Prüfung der zugrundeliegenden Fallkonstellation bejaht und gab in ihrer erstinstanzlichen Verfügung den Beschwerden der Beschwerdeführer vollumfänglich statt. Überdies stellte die DSS in einem Fall neben den geltend gemachten Verletzungen der Datenschutzbestimmungen amtswegig einen Verstoss gegen Art. 7 und 32 DSGVO durch die Beschwerdegegnerin erster Instanz fest.

Gegen die Verfügungen der DSS legte die Beschwerdegegnerin erster Instanz Beschwerde bei der VBK ein und machte hierbei neben ihren Beschwerdepunkten zu den von der DSS in ihrer Verfügung festgestellten Datenschutzverstössen als Beschwerdepunkte insbesondere auch eine Verletzung des Rechts auf Gehör als Folge der Anonymität der Beschwerdeführer geltend. Auch machte sie den Ersatz der Partei- und Verfahrenskosten geltend.

Die VBK unterbrach das Verfahren und legte die Frage der Möglichkeit der anonymen Beschwerdeführung dem EFTA-Gerichtshof als Vorfrage vor. Ebenfalls von der VBK als Vorfrage dem EFTA-Gerichtshof unterbreitet war die Frage, 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 darf. Die DSS hat zu diesem Urteil in ihrem letzten Jahresbericht zum Berichtsjahr 2020 unter Punkt 5.2.3 (S. 35) bereits berichtet.

In seinem Urteil vom 10. Dezember 2020 verneinte der EFTA-Gerichtshof die Kostenersatzpflicht in Beschwerdeverfahren vor weiterführenden Rechtsmittelinstanzen gemäss Art. 78 DSGVO. Der EFTA-Gerichtshof stellte in seinem Urteil klar, dass einen Be-

schwerdeführer erster Instanz, der ohne sein Zutun zum Beklagten (Verfahrenspartei) in einem Beschwerdeverfahren nach Art. 78 Abs. 1 DSGVO wird, keine Kostenersatzpflicht trifft. Zur anonymen Beschwerdeführung führte der EFTA-Gerichtshof aus, dass nicht in jedem Fall die Offenlegung der Identität des Beschwerdeführers gegenüber dem Verantwortlichen der Datenverarbeitung (sprich dem Unternehmen) erforderlich sei und erläuterte die Grundsätze, welche die verantwortliche Stelle (Aufsichtsbehörde) bei der Entscheidung der Offenlegung bzw. Nichtoffenlegung der personenbezogenen Daten leiten sollten. Der EFTA-Gerichtshof führte hierbei aus, dass bei der Beurteilung, ob es erforderlich ist, die Identität von Beschwerdeführern gegenüber anderen Parteien offenzulegen, ein Gleichgewicht zwischen den Interessen, Rechten und Freiheiten der betroffenen Personen und dem Recht der Parteien auf Verteidigung und faires Verfahren zu wahren sei. Die Anonymität sei zu verneinen, wenn der Verantwortliche seiner Möglichkeit beraubt würde, den genauen Sachverhalt zum Vorbringen des Beschwerdeführers zu ermitteln und von seinen Verteidigungsrechten Gebrauch zu machen. Vom EFTA-Gerichtshof damit angesprochen ist auch die Ausübung des Rechts auf wirksamen gerichtlichen Rechtsbehelf und ein ordnungsgemässes Verfahren entsprechend von Art. 58 Abs. 4 DSGVO. Der EFTA-Gerichtshof legte weiter dar, dass eine Offenlegung der Identität des Beschwerdeführers für die wirksame Ausübung des Verteidigungsrechts unter Umständen dann nicht erforderlich sei, wenn der Untersuchung und der darauf basierenden Entscheidung der Aufsichtsbehörde eine standardisierte und gleichartige Datenverarbeitung für eine unbestimmte Anzahl betroffener Personen zugrunde liegt oder mehrere gleichartige Beschwerden Untersuchungsgegenstand sind. Mit dieser Feststellung hatte der EFTA-Gerichtshof wohl auch die Datenverarbeitungen der Gegenstand bildenden Beschwerden im Blick.

Nach Vorliegen des EFTA-Gerichtshofurteils vom 10. Dezember 2020 erliess die VBK im Frühjahr 2021 ihre Entscheidung in den unterbrochenen Verfahren. Sie entschied in beiden Fällen, die Verfügung der DSS aufzuheben und die Verwaltungssache an die DSS zurückzuverweisen. Diese habe das Verfahren neu durchzuführen und die Identität des Beschwerdeführers erster Instanz dem Verantwortlichen gegenüber offenzulegen. Auf eine materiell-rechtliche Prüfung des Falles betreffend der von der Beschwerdegegnerin erster Instanz in ihrer Beschwerde an die VBK vorgebrachten Beschwerdepunkte trat die VBK nicht ein.

Die VBK begründete ihre Entscheidung der Zurückverweisung des Verfahrens an die DSS damit, dass die Beschwerdegegnerin erster Instanz durch die Nichtoffenlegung der Identität der betroffenen Personen (Beschwerdeführer) in ihrer Fähigkeit, von ihren Verteidigungsrechten Gebrauch zu machen, eingeschränkt worden sei. Ein schutzwürdiges Interesse der betroffenen Person auf Nichtoffenlegung ihrer Identität sei von der DSS nicht dargelegt worden. Gegen diesen Entscheid der VBK legte die DSS beim VGH Beschwerde ein. Zudem legte auch die Beschwerdegegnerin erster Instanz Beschwerde beim VGH ein.

Der VGH prüfte die Möglichkeit der anonymen Beschwerdeführung im gegenständlichen Fall unter Bezugnahme auf die der Beschwerde zugrundeliegenden Datenverarbeitungen in Verbindung mit den diesbezüglichen Leitlinien gemäss EFTA-Gerichtshofurteil. Der VGH stellte fest, dass es sich um standardisierte und gleichartige Datenverarbeitungen handelte, die für eine unbestimmte Anzahl von betroffenen Personen identisch zur Anwendung gelangten. Dies führe dazu, dass die von den Beschwerdeführern dargelegten mutmasslichen Datenschutzverletzungen losgelöst von einer konkreten betroffenen Person geprüft werden könnten und die Beschwerdegegnerin erster Instanz auch ohne Offenlegung der Identität des Beschwerdeführers die der Beschwerde zugrundeliegende Sachlage prüfen und ihre Verteidigungsrechte wirksam wahrnehmen könne. Mit dieser Begründung verwarf der Verwaltungsgerichtshof die gegenteilige Argumentation und Begründung, welche die VBK ihrer Entscheidung zugrunde gelegt hatte. Der VGH verwies den Fall zurück an die VBK zur weiteren materiellrechtlichen Behandlung der Beschwerde.

VGH-Urteil 2020/050 (Fall 3) und VGH-Urteil 2020/051 (Fall 4)

Die Beschwerdefälle zu VGH 2020/050 und VGH 2020/051 sind aufgrund weitgehend gleicher Beschwerdekonstellation und gleichen Datenverarbeitungen in weiten Teilen identisch. Für die nachstehende Falldarstellung wurde der Fall zu VGH 2020/051 gewählt. In diesem Fall hatte die VBK die Beschwerde der Beschwerdegegnerin erster Instanz gegen die Verfügung der DSS in allen Punkten abgewiesen und die Verfügung der DSS vollumfänglich bestätigt.

In ihrer Verfügung hatte die DSS festgestellt, dass nicht für alle Verarbeitungsvorgänge von personenbezogenen Daten der Beschwerdeführer eine Rechtsgrundlage gemäss Art. 6 Abs. 1 DSGVO vorliegt und damit die Verarbeitung der personenbezogenen Daten durch die Beschwerdegegnerin teilweise gegen Art. 5 Abs. 1 Bst. a i.V.m. Art. 6 Abs. 1 DSGVO verstossen hat. Überdies stellte sie neben den geltend gemachten Verletzungen der Datenschutzbestimmungen amtswegig

einen Verstoss gegen Art. 7 und 32 DSGVO durch die Beschwerdegegnerin erster Instanz fest.

Gegen die Entscheidung der VBK erhob die Beschwerdegegnerin erster Instanz nachfolgend Beschwerde an den VGH, der die Beschwerde der Beschwerdegegnerin erster Instanz abwies und die Entscheidung der VBK bestätigte.

Die Beschwerdegegnerin erster Instanz brachte in ihrer Beschwerde an den VGH eine Reihe von Beschwerdegründen formeller und materieller Natur vor. Die DSS beschränkt sich im Rahmen dieses Tätigkeitsberichts auf einige aus Datenschutzsicht relevante Beschwerdegründe. Die Beschwerdegegnerin erster Instanz hatte in ihrer Beschwerde an den VGH geltend gemacht, dass die DSS für den Beschwerdefall unzuständige Behörde gewesen sei und damit die Verfügung der DSS am formellen Mangel der Unzuständigkeit leide. Die Beschwerdeführer hätten sich initial an die Datenschutz-Aufsichtsbehörde ihres gewöhnlichen Aufenthaltsorts gewandt. Diese wäre für den Fall in der Folge auch zuständige Behörde gewesen. Auch die datenverarbeitende Stelle, die im Beschwerdefall involviert sei, habe ihren Sitz in Deutschland, was die Zuständigkeit der für diese zuständige deutsche Aufsichtsbehörde begründet hätte. Der VGH entkräftete das Beschwerdevorbringen der Beschwerdegegnerin erster Instanz betreffend die fehlende örtliche Zuständigkeit der DSS unter Zugrundelegung von Art. 77 DSGVO einerseits und Art. 56 DSGVO andererseits. Art. 77 DSGVO erlaubt es einer betroffenen Person, ihre Beschwerde im Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmasslichen Verstosses einzubringen. Ein Beschwerdeführer hat also unter den in Art. 77 DSGVO gegebenen Möglichkeiten die Wahl, bei welcher Datenschutz-Aufsichtsbehörde er seine Beschwerde einbringen will. Im gegebenen Fall hatten die Beschwerdeführer zunächst das Gespräch mit der für ihren gewöhnlichen Aufenthaltsort zuständigen Datenschutz-Aufsichtsbehörde gesucht und in der Folge ihre Beschwerde bei der DSS eingebracht. Die DSS war für die Beschwerdegegnerin als liechtensteinisches Unternehmen zuständige Aufsichtsbehörde. Der VGH verweist zudem auf Art. 56 DSGVO, der – wie er ausführt – zu keinem anderen Ergebnis geführt hätte. Würden die Beschwerdeführer ihre Beschwerde bei der zuständigen Aufsichtsbehörde ihres gewöhnlichen Aufenthaltsortes eingebracht haben, wäre diesfalls die DSS entsprechend von Art. 56 Abs. 1 DSGVO «federführende» Behörde für die Beschwerde gewesen und die deutsche Aufsichtsbehörde «beteiligte» Behörde, was, wie der VGH zurecht feststellt, letztlich zu gleichem Ergebnis geführt hätte. Nach Art. 56 Abs. 1 DSGVO ist die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen gemäss dem Verfahren nach Art. 60 DSGVO die für die durchgeführte, grenzüberschreitende Datenverarbeitung zuständige federführende Aufsichtsbehörde. Für die Beschwerdegegnerin als liechtensteinisches Unternehmen hätte sich auch hier die DSS mit dem Beschwerdefall als federführende Behörde zu befassen gehabt und hätte die Verfügung als federführende Behörde erlassen.

Die Beschwerdegegnerin erster Instanz machte in ihrer Beschwerde an den VGH auch geltend, dass der zeitliche Anwendungsbereich der DSGVO für den gegenständlichen Beschwerdefall nicht eröffnet sei. Die Beschwerdegegnerin erster Instanz rügte, dass der massgebliche Sachverhalt, welcher der Beschwerde zugrunde gelegen hatte, bei Inkrafttreten der DSGVO bereits abgeschlossen gewesen sei. Der VGH entkräftete dies gegründet auf den für den gegenständlichen Fall anwendbaren Art. 3 Abs. 2 Bst. a DSGVO. Die letzte massgebende Datenverarbeitung fiel nämlich in die Zeit vom 25. Mai 2018 und 20. Juli 2018, eine Zeitspanne, in der Liechtenstein in Bezug zur DSGVO noch als Drittstaat galt. Die Datenverarbeitung der Beschwerdegegnerin erster Instanz stand entsprechend von Art. 3 Abs. 2 Bst. a DSGVO im Zusammenhang damit, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, womit Art. 3 Abs. 2 Bst. a DSGVO eröffnet war und für die Beschwerdegegnerin erster Instanz in der fraglichen Zeitspanne die DSGVO anwendbar war.

Die Beschwerdegegnerin erster Instanz rügte in ihrer Beschwerde an den VGH des Weiteren, die DSS habe im gegenständlichen Beschwerdeverfahren eine Vermischung von kontradiktorischem Verfahren und amtswegigem Verfahren vorgenommen. Die DSS hatte unter anderem amtswegig geprüft, ob die technischen und organisatorischen Massnahmen im Einklang mit der DSGVO standen. Der VGH bejahte die Möglichkeit der amtswegigen Prüfung datenschutzrechtlicher Vorgaben gestützt auf Art. 57 Abs. 1 Bst. h DSGVO. Art. 57 Abs. 1 Bst. h DSGVO erlaubt es Datenschutz-Aufsichtsbehörden, Untersuchungen aus eigenem Antrieb durchzuführen und damit im Zusammenhang mit einer Beschwerde auch anderen Ansprüchen und Gegenständen, welche die betroffene Person in ihrer Beschwerde vor der Datenschutz-Aufsichtsbehörde selbst nicht vorgebracht hat, zu untersuchen. Der VGH bekräftigte, dass Gleiches auch der EFTA-Gerichtshof in seinem Urteil vom 10. Dezember 2020 befand und auch die vorliegende Literatur dieses Ergebnis klar unterstreiche.

Die Beschwerdegegnerin erster Instanz hatte in ihrer Beschwerde an den VGH auch vorgebracht, dass die Verfügung der DSS in verschiedenen Punkten am Bestimmtheitsgrundsatz mangle. In Bezug auf Art. 32 DSGVO hatte die DSS Mängel hinsichtlich der von der Beschwerdegegnerin erster Instanz implementierten TOM festgestellt und die festgestellten Mängel in ihrer Verfügung umfassend dargelegt. Um die Datenverarbeitungen in Einklang mit der DSGVO zu bringen, hatte die DSS diesbezüglich Anweisungen entsprechend von Art. 32 DSGVO erlassen, wobei der Zweck und das Ziel der angeordneten TOM von der DSS klar festgelegt wurden. Die konkret zu ergreifenden TOM sollten die Zweckerreichung garantieren und entsprechend von Art. 32 DSGVO zu erfolgen haben. Die Beschwerdegegnerin erster Instanz rügte, die DSS hätte die Anordnung präzisieren und konkret beschreiben müssen, welche TOM zu ergreifen und wie diese konkret umzusetzen seien. Der VGH verneinte eine Verletzung des Bestimmtheitsgebots mit der Begründung, dass weder Art. 57 noch Art. 58 DSGVO die Aufsichtsbehörde verpflichten, dem Verantwortlichen konkrete TOM vorzuschreiben. Der VGH führte weiter aus, dass es für den Verantwortlichen nur eindeutig erkennbar sein müsse, welche Mängel er unter Massgabe des zu erreichenden Ziels zu beseitigen habe. Der VGH führte aus, dass die DSS in ihrer Verfügung die Mängel der implementierten TOM klar aufgezeigt und auch den Weg dargelegt habe, wie die Mängel beseitigt werden können.

VGH-Urteil zu VGH 2021 / 014 (Fall 5)

Dem vor dem VGH zu VGH 2021 / 014 entschiedenen Fall lag in erster Instanz eine Beschwerde an die DSS zugrunde, in welcher der Beschwerdeführer vorbrachte, unangefordert einen Newsletter vom Amt für Statistik erhalten zu haben. Das Amt für Statistik als Verantwortliche für den Newsletter gemäss Art. 4 Zif. 7 DSGVO habe ihm auf entsprechendes Auskunftsgesuch gemäss Art. 15 DSGVO in der Folge beauskunftet, dass er sich für den Erhalt des Newsletters registriert und damit seine Einwilligung zum Erhalt von Newslettern gegeben habe. Der Beschwerdeführer seinerseits behauptete in seiner Beschwerde, dass er sich für den Erhalt des fraglichen Newsletters nicht registriert habe bzw. zu keinem Zeitpunkt in den Erhalt eines solchen eingewilligt habe und bemängelte damit, dass es für die Verarbeitung seiner Daten an einer Rechtsgrundlage gemäss Art. 6 Abs. 1 DSGVO fehlte. Im Zuge der Sachverhaltsermittlung durch die DSS im erstinstanzlichen Verfahren stellte sich heraus, dass das Anmeldeverfahren zu Newslettern der LLV missbrauchsanfällig war, was es in der zu diesem Zeitpunkt gegebenen Ausgestaltung insbesondere erlaubte, dass eine dritte unbefugte Person einen Newsletter für eine andere Person bestellen konnte, deren E-Mail-Adresse sie kannte. Eine Analyse des konkreten Beschwerdefalles ergab, dass tatsächlich eine dritte Person, deren Identität nicht eruiert werden konnte, die Newsletter-Registrierung unter Eingabe der E-Mail-Adresse des Beschwerdeführers für denselben vorgenommen hatte. Die Bestellung eines Newsletters für eine andere Person mittels Eingabe ihrer E-Mail-Adresse war möglich, weil das Newsletter-Registrierungsprozedere der LLV zum Zeitpunkt des Eingangs der Beschwerde technisch noch nicht als Double-Opt-In-Verfahren ausgestaltet war. Beim Double-Opt-In-Verfahren wird einer Person, die sich mit ihrer E-Mail-Adresse für einen Newsletters registriert, zeitnah mit einer Bestätigungs-E-Mail die Möglichkeit gegeben, die getätigte Registrierung zu prüfen und – meist via Hyperlink – zu bestätigen oder diese gegebenenfalls zu berichtigen bzw. abzubrechen. Erst nach einer solchermassen erfolgten Bestätigung der Registrierung ist die Newsletter-Anmeldung abgeschlossen. Noch im Laufe des erstinstanzlichen Verfahrens wurde das fehlende Double-Opt-In-Verfahren in das Newsletter-Registrierungsprozedere der LLV implementiert, womit eine missbräuchliche Eingabe von E-Mail-Adressen fortan nicht mehr möglich war. Die Anmeldung eines Newsletters muss seither von den Abonnenten des Newsletters zusätzlich über einen Hyperlink in einer dafür an den Newsletter-Empfänger zugesandten E-Mail bestätigt werden.

Die DSS stellte in ihrer Verfügung fest, dass das Beschwerdevorbringen des Beschwerdeführers zum Zeitpunkt der Beschwerdeeinbringung berechtigt war, insofern die Verarbeitung seiner personenbezogenen Daten aufgrund Fehlens einer Rechtsgrundlage gemäss Art. 5 Abs. 1 Bst. a DSGVO i.V.m. Art. 6 Abs. 1 DSGVO (mangelhafte Einwilligung) unrechtmässig war und gab der Beschwerde statt. Die DSS stellte gleichzeitig in der Verfügung fest, dass im laufenden Verfahren die genannte Rechtsverletzung durch Implementierung eines zweistufigen Einwilligungsprozesses (Double-Opt-In-Verfahren) vollumfänglich behoben wurde.

Der Beschwerdeführer erhob gegen die Verfügung der DSS Beschwerde an die VBK, mit der er die Verfügung der DSS vollumfänglich bekämpfte und den Antrag stellte, die VBK wolle seiner Beschwerde Folge geben und die Angelegenheit zur neuerlichen Entscheidung an die DSS zurückverweisen. Ebenso brachte er verschiedene Eventualanträge ein. In seiner Beschwerde machte der Beschwerdeführer die Verletzung von Formvorschriften (elektronische Signatur der Verfügung, Mängel in der Zustellung der Verfügung),

Verletzung der Unparteilichkeit, nicht abschliessende Prüfung in materiell-rechtlicher Hinsicht und unrichtige rechtliche Beurteilung geltend.

Die VBK wies die Beschwerde des Beschwerdeführers gegen die Verfügung der DSS aufgrund Nichtvorliegen der Beschwer gemäss Art. 92 Abs. 1 LVG ab und bestätigte die angefochtene Verfügung der DSS. Beschwer eines Beschwerdeführers liegt dann vor, wenn der Beschwerdeführer durch einen Hoheitsakt persönlich einen Nachteil erfährt (Beschwer) und dieser durch die beantragte Aufhebung eliminiert werden kann (aktuelles Rechtsschutzbedürfnis). Die VBK sah nach Prüfung des Falles eine Beschwer des Beschwerdeführers als nicht gegeben und erkannte in ihrer Entscheidung, dass gestützt darauf die Beschwerde des Beschwerdeführers vollumfänglich abzuweisen und auf das weitere Vorbringen des Beschwerdeführers nicht einzugehen war.

Gegen die Entscheidung der VBK erhob der Beschwerdeführer in weiterer Folge Beschwerde an den VGH und brachte hier vor, dass die Verneinung der Beschwer durch die VBK, und die daraus gefolgerte schlichte Abweisung sämtlicher Anträge durch die VBK, gegen die elementare Begründungspflicht verstossen habe.

Der VGH seinerseits gelangte nach Prüfung der vorgelegten Akten zum Ergebnis, dass es dem Beschwerdeführer bei seiner Beschwerde an die VBK an einem Rechtsschutzinteresse fehlte und dass die VBK zurecht nicht auf das weitere Beschwerdevorbringen in seiner Beschwerde einzugehen hatte und damit die Begründungspflicht nicht verletzt habe. Der VGH bestätigte mit seinem Urteil damit die Entscheidung der VBK und wies die Beschwerde des Beschwerdeführers zurück.

5.3 Meldung von Datenschutzverletzungen gemäss Art. 33 DSGVO

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

2021 erhielt die DSS 55 Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO, wovon in 10 Fällen die betroffenen Personen über die Datenschutzverletzung benachrichtigt wurden (Art. 34 DSGVO). Dies bedeutete eine signifikante Zunahme im Vergleich zum Vorjahr, in dem lediglich 20 Meldungen nach Art. 33 DSGVO erfolgten. Die Zunahme der Meldungen ist zudem ein Trend, den auch andere europäische Datenschutz-Aufsichtsbehörden verzeichnen. Insgesamt zeigten die Meldungen, dass es für die Ver-

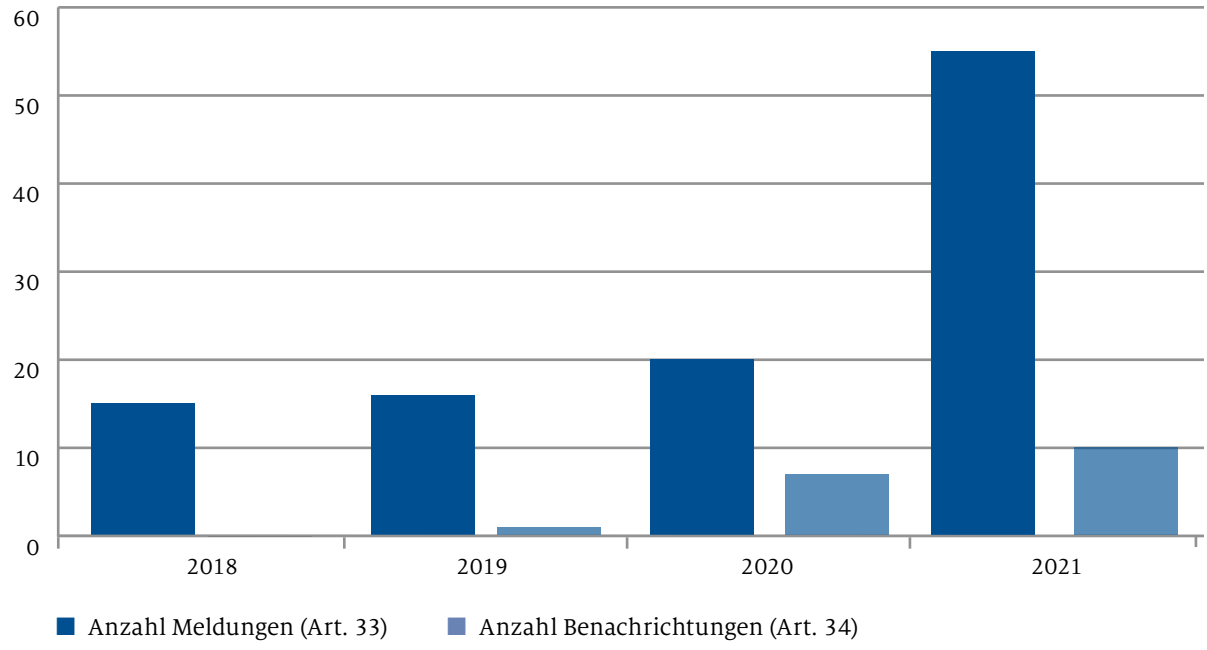


Abbildung 6: Anzahl der gemeldeten Datenschutzverletzungen pro Jahr

antwortlichen 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. Nicht selten sind einfachste und bereits seit langem bekannte Sicherheitsmängel bzw. -fehler der Grund für die Datenpannen, weshalb davon auszugehen ist, dass die Dunkelziffer noch um einiges höher ist.

Nicht selten bestand im Zusammenhang mit Art. 33 Meldungen eine gewisse Unsicherheit bei den Verantwortlichen bezüglich des konkreten Zeitpunktes, ab dem eine solche Meldung zu erfolgen hat. Dies bezog sich vor allem auf die Frage, ob die Identifizierung einer IT-Schwachstelle per se bereits als Verpflichtung zu einer Meldung einzustufen ist. Dazu konnte von der DSS ausgeführt werden, dass im Falle von konkreten Hinweisen für eine technische Kompromittierung und der Feststellung, dass Risiken für die betroffenen Personen nicht belastbar ausgeschlossen werden können, eine Meldepflicht nach Art. 33 DSGVO bereits eröffnet ist. Die Feststellung, dass personenbezogene Daten tatsächlich widerrechtlich verarbeitet wurden, ist nicht erforderlich und die Meldepflicht besteht bereits im Zeitpunkt einer solchen Möglichkeit.

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.

«Im Berichtsjahr unterstützte die DSS die Landesverwaltung unter anderem bei der Erarbeitung einer Risikobeurteilung im Zusammenhang mit dem Einsatz von Microsoft Online Services.»

6. Mitarbeit in Arbeitsgruppen und Projekten der Landesverwaltung

6.1 Risikobetrachtung im Zusammenhang mit dem Einsatz von Microsoft Online Services

Im Berichtsjahr unterstützte die DSS die Landesverwaltung unter anderem bei der Erarbeitung einer Risikobeurteilung im Zusammenhang mit dem Einsatz von Microsoft Online Services durch das Aufzeigen der damit zusammenhängenden Compliance-Risiken im Bereich Datenschutz. Denn bei der Verwendung von Cloud-Services kann es durchaus vorkommen, dass die Teile eines bestimmten Verarbeitungsvorgangs in unterschiedlichen weltweit verstreuten Rechenzentren verarbeitet werden. Um das Compliance-Risiko im Zusammenhang mit dem Datentransfer, insbesondere in die USA, beurteilen zu können, waren vor allem die Datenschutzregelungen und Vereinbarungen zwischen Microsoft und der Landesverwaltung bei der Nutzung der Microsoft-Onlinedienste zu konsultieren. Ebenso sind durch die Harmonisierung des Datenschutzrechts im EU / EWR-Raum Entscheidungen von Datenschutz-Aufsichtsbehörden anderer Mitgliedsstaaten für die Beurteilung von Sachverhalten in Liechtenstein relevant. Doch aktuell wird die Verwendung von Microsoft Cloud Services unter den europäischen Datenschutzbehörden sehr kontrovers diskutiert. Wenngleich einzelne europäische Datenschutzbehörden den Entschluss gefasst haben, die Nutzung von Microsoft in der öffentlichen Verwaltung zu untersagen, bleiben dies Ausnahmen. Daneben befinden sich zahlreiche europäische Gesetzgebungsinitiativen in Ausarbeitung, welche direkten Einfluss auf die Datenverarbeitungen mit Microsoft Online Services durch die Landesverwaltung haben werden. Diese Gesetzgebungsvorhaben sind zu beobachten.

6.2 OECD Confidentiality Assessment

Die OECD hat 2021 in Liechtenstein turnusgemäss ein Confidentiality Assessment durchgeführt. Dabei wurden verschiedene Bereiche, die in Zusammenhang mit dem von der OECD regulierten, automatischen Informationsaustausch in Steuersachen (AIA) stehen, wie AIA-Datenzyklus, IT-Sicherheit, entsprechende Personalauswahl, Gebäudesicherheit etc. genau durchleuchtet und beurteilt. Einige dieser Bereiche unterfallen jedoch auch Regulierungen durch das Datenschutzrecht und der Aufsicht durch die DSS. Entsprechend hat die DSS die Steuerverwaltung und das Amt für Informatik gezielt unterstützt und den OECD-Experten im Rahmen von deren (ausnahmsweise digital via Videokonferenz durchgeführten) Vor-Ort-Besuchs die unter ihren Einfluss fallenden datenschutzrechtlichen Regelungen in Liechtenstein vorgestellt.

6.3 Ratifikation Konvention 108+

Die DSS hat im Berichtsjahr weiterhin das Amt für Auswärtige Angelegenheiten beim Ratifikationsprozess des Änderungsprotokolls zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) des Europarats unterstützt. Das Übereinkommen wurde kürzlich mittels eines Änderungsprotokolls modernisiert und insbesondere an die heutigen informations- und kommunikationstechnologischen Möglichkeiten der Datenverarbeitung angepasst. 2021 war die DSS erneut in vorbereitende Arbeiten für den Bericht und Antrag an den Landtag involviert. Die formelle Ratifikation des Änderungsprotokolls durch Liechtenstein wird für 2022 erwartet.

6.4 Multi-Stakeholder-Befragung CAHAI

Des Weiteren wurde das Amt für Auswärtige Angelegenheiten im Berichtsjahr von der DSS auch bei der Beantwortung eines Fragebogens des Ad hoc Committee on Artificial Intelligence (CAHAI) des Europarats unterstützt, welches eine Multi-Stakeholder-Befragung zum Thema künstliche Intelligenz durchführte. Damit wollte das CAHAI – in Hinblick auf die mögliche Schaffung eines verbindlichen Rechtsrahmens – von öffentlichen wie auch privaten Akteuren Informationen für eine Machbarkeitsstudie wie auch zu regulatorischen Optionen im Bereich der künstlichen Intelligenz sammeln.

6.5 VwEG-Kommission

Gemäss Art. 13 des Gesetzes vom 6. Dezember 2018 über das Verzeichnis der wirtschaftlichen Eigentümer inländischer Rechtsträger (VwEG) hat die DSS Einsitz in der VwEG-Kommission. Im Berichtsjahr wurde ein Antrag gemäss Art. 12 VwEG betreffend die Offenlegung von Daten an Dritte an das Amt für Justiz gestellt. Der Antrag wurde von der VwEG-Kommission im November entschieden.

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

7. Internationale Zusammenarbeit

7.1 Europäischer Datenschutzausschuss

Eine der Hauptaufgaben des Europäischen Datenschutzausschusses (EDSA) ist der Erlass von Leitlinien, aber auch der Abgabe von Empfehlungen und Stellungnahmen u.ä., die der einheitlichen Auslegung und Anwendung der DSGVO dienen. Die Grundlagen für all diese Dokumente des Ausschusses werden in insgesamt zwölf thematischen Arbeitsgruppen (Expert Subgroups) geschaffen, welche die Dokumente für die Abstimmung im Ausschuss vorbereiten. Wie bereits im Vorjahr konnte die DSS auch 2021 an den meisten Sitzungen der Arbeitsgruppen teilnehmen und dort, wo es für Liechtenstein von Bedeutung ist, aktiv mitarbeiten. Die DSS nahm ausserdem an sämtlichen 15 Plenarsitzungen im Berichtjahr teil.

Der EDSA hat im Jahr 2021 auf Grundlage des Art. 64 Abs. 1 DSGVO insgesamt 33 **Stellungnahmen** zu Vorlagen von nationalen Datenschutz-Aufsichtsbehörden abgegeben. Darunter fielen:

- fünf Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Überwachung von Verhaltensregeln gemäss Art. 41 DSGVO (Malta, Norwegen, Slowakei, Tschechische Republik, Ungarn);
- sieben Stellungnahmen zum Entwurf der Akkreditierungsanforderungen für eine Stelle zur Zertifizierung gemäss Art. 43 Abs. 3 DSGVO (Belgien, Lettland, Litauen, Norwegen, Portugal, Rumänien, Ungarn);
- zwei Stellungnahmen zu Entwürfen von Verhaltensregeln im Cloud-Services-Bereich (Belgien, Frankreich);
- eine Stellungnahme zum Entwurf von Standardvertragsklauseln gemäss Art. 28 Abs. 8 DSGVO (Litauen);
- 18 Stellungnahmen zu verbindlichen internen Datenschutzvorschriften (zwei zu BDO; Carrier; zwei zur CGI Group; zwei zur COLT Group; Elanders Group; zwei zur Internet Initiative Japan Group; zwei zur Kumon Group; zwei zur Luxoft Group; zwei zur Oregon Tool, Inc. (formerly «Blount»); Otis; Saxo Bank Group).

Daneben hat der EDSA 2021 auch zwei Stellungnahmen gemäss Art. 64 Abs. 2 DSGVO erlassen, welche eine Verwaltungsvereinbarung zwischen Behörden zum internationalen Datentransfer (Frankreich) sowie die genaue Auslegung des Art. 58 Abs. 2 Bst. g DSGVO betrafen (Ungarn).

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

- Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0 (EDPB Guidelines 01 / 2020);
- Massgeblicher und begründeter Einspruch im Sinne der Verordnung (EU) 2016 / 679, Version 2.0 (EDPB Guidelines 09 / 2020);
- Gezielte Ansprache von Nutzer:innen sozialer Medien, Version 2.0 (EDPB Guidelines 8 / 2020);
- Virtuelle Sprachassistenten, Version 2.0 (EDPB Guidelines 02 / 2021);
- Begriffe «Verantwortlicher» und «Auftragsverarbeiter» in der DSGVO, Version 2.0 (EDPB Guidelines 07 / 2020);
- Beschränkungen nach Artikel 23 DSGVO, Version 2.0 (EDPB Guidelines 10 / 2020).

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

- Beispiele für die Meldung von Datenschutzverletzungen (EDPB Guidelines 01 / 2021);
- Assessment von Zertifizierungskriterien (Anhang zu den Leitlinien 1 / 2018 über die Zertifizierung und die Festlegung von Zertifizierungskriterien gemäss den Artikeln 42 und 43 der Verordnung);
- Anwendung von Artikel 65(1)(a) DSGVO (EDPB Guidelines 03 / 2021);
- Verhaltensregeln als Transferinstrument (EDPB Guidelines 04 / 2021);
- Zusammenspiel zwischen der Anwendung von Artikel 3 und den Bestimmungen über internationale Datentransfers gemäss Kapitel V der DSGVO (Guidelines 05 / 2021).

Im Berichtsjahr wurden vom EDSA ausserdem drei **Empfehlungen** zu folgenden Themen erlassen:

- Referenzgrundlage für den Begriff «Angemessenheit» in der Richtlinie zum Datenschutz bei der Strafverfolgung (Recommendations 01 / 2021);
- Rechtsgrundlage für die Speicherung von Kreditkartendaten ausschliesslich zum Zweck der Erleichterung weiterer Online-Transaktionen (Recommendations 02 / 2021);
- Massnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0 (Recommendations 01 / 2020).

7.1.1 Arbeitsgruppen

Die spezielle Arbeitsgruppe (Task Force) des EDSA zu Bussgeldern gemäss DSGVO (*Taskforce Fining)* befasst sich mit der konkreten Berechnung solcher Bussgelder und strebt europaweit eine möglichst einheitliche Herangehensweise an. 2021 setzte die Task Force ihre Arbeit an Leitlinien des EDSA fort, welche die Berechnung von Bussgeldern methodisch systematisieren und europaweit harmonisieren sollen. Der Entwurf der Leitlinien ist schon weit fortgeschritten und soll 2022 endgültig verabschiedet werden.

In der Arbeitsgruppe, welche sich mit der Zusammenarbeit der Aufsichtsbehörden befasst (*Cooperation Subgroup*), wurden im Berichtsjahr insbesondere die Leitlinien zum Kooperationsverfahren bei grenzüberschreitenden Beschwerden gemäss Art. 60 DSGVO weiter ausgearbeitet und in grossen Teilen bereits vom EDSA verabschiedet. 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. Zusätzlich wurden 2021 von dieser Arbeitsgruppe auch Leitlinien zum massgeblichen und begründeten Einspruch einer betroffenen Aufsichtsbehörde in solch grenz-überschreitenden Verfahren mit mehreren beteiligten Behörden fertiggestellt und angenommen. Und schliesslich wurden die Arbeiten an internen Leitlinien zur Möglichkeit der gütlichen Streitbeilegung im Rahmen grenzüberschreitender Verfahren fortgeführt.

Diejenige Arbeitsgruppe des EDSA, welche sich mit der möglichst einheitlichen Durchsetzung der Bestimmungen der DSGVO in den Mitgliedstaaten befasst (*Enforcement Subgroup*), war im Berichtsjahr erneut mit der Durchführung eines Streitbeilegungsverfahrens 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 hat die Arbeitsgruppe auch eine Stellungnahme des EDSA gemäss Art. 64 Abs. 2 DSGVO vorbereitet, da eine Aufsichtsbehörde die Klärung der rechtlichen Begründung von behördlichen Löschanordnungen verlangte. Und schliesslich wurden von der Arbeitsgruppe die Arbeiten an generellen Leitlinien zum Verfahren des Streitbeilegungsmechanismus gemäss Art. 65 DSGVO fortgeführt und der Teil zum Art. 65 Abs. 1 Bst. a DSGVO bereits vom EDSA verabschiedet. Die Erarbeitung der weiteren Teile dieser Leitlinien ist für 2022 vorgesehen.

Daneben hat die Arbeitsgruppe auch ein so genanntes Coordinated Enforcement Framework ins Leben gerufen, im Rahmen dessen jedes Jahr von den europäischen Aufsichtsbehörden gemeinsam ein bestimmtes datenschutzrechtliches Thema europaweit untersucht wird. Die erste solche Coordinated Action ist nun für 2022 vorgesehen und wird sich mit der Nutzung von Cloud-basierten Services durch öffentliche Stellen befassen.

Die thematische Arbeitsgruppe zu Finanzangelegenheiten des EDSA (*Financial Matters Subgroup*) hat im Berichtsjahr insbesondere Empfehlungen zur rechtlichen Grundlage der Speicherung von Kreditkartendaten im Rahmen von Online-Shops erlassen. Darüber hinaus hat sie diverse Stellungnahmen und kleinere Beiträge zu regulatorischen Vorhaben der Kommission, der Europäischen Zentralbank oder auch zu im EDSA behandelten Themen wie Bekämpfung von Geldwäscherei und Terrorismusfinanzierung, Digitaler Euro oder FATCA erarbeitet.

Die Arbeitsgruppe zu Fragen bezüglich Datenübermittlungen in Drittstaaten *(International Transfer Subgroup)* hat die im Vorjahr aufgenommenen Arbeiten an einer Richtline zur Nutzung von Verhaltensregeln (Codes of Conduct) wie auch Zertifizierungen als geeignete Garantien für internationale Datentransfers weitergeführt. Aufgrund differenzierter und übergreifender Fragestellungen, wie auch aufgrund der grundsätzlichen Komplexität der Thematik konnte die Richtlinie zu Zertifizierungen als geeignete Garantie im Berichtsjahr noch nicht finalisiert und verabschiedet werden. Auch das Überarbeiten der Hilfestellungen für BCR-Verfahren (Working-Papers), welches schon im Vorjahr aufgegriffen wurde, konnte im Berichtsjahr noch nicht ganz abgeschlossen werden. Ausschlaggebend hierfür sind umfassende Diskussionen zu einzelnen Punkten, insbesondere aber auch die Aufnahme von Voraussetzungen bezüglich ergänzender Massnahmen (Supplementary Measures), welche nach dem «Schrems II»-Urteil für Datentransfers in Drittstaaten allenfalls zu implementieren sind. In Zusammenhang mit Datentransfers in die USA beobachtet die Arbeitsgruppe auch das Bestreben einer Etablierung eines Nachfolgesystems zum EU-U.S. Privacy Shield. Hierzu wurden im Berichtsjahr jedoch erst erste Analysen und Verhandlungen aufgenommen. Auch Datenverarbeitungen in Zusammenhang mit dem FATCA-Abkommen rückten in den Fokus der Arbeitsgruppe und werden diese wohl auch im nächsten Jahr beschäftigen. Abschliessend ist noch eine Erfolgsmeldung aufzuführen: Die schon seit Jahren diskutierte, genaue De-

finition eines internationalen Datentransfers konnte im Berichtsjahr mit der Verabschiedung der Leitlinien zum Zusammenspiel zwischen Artikel 3 und Kapitel V DSGVO abgeschlossen werden. Sie stellen das Zusammenspiel zwischen dem räumlichen Anwendungsbereich der DSGVO (Art. 3) und den Bestimmungen zum internationalen Datentransfer in Kapitel V klar. Dies soll die Verantwortlichen und ihre Auftragsverarbeiter im EU / EWR-Raum bei der Feststellung unterstützen, ob es sich bei einem Verarbeitungsprozess um eine internationale Übermittlung handelt. Es soll damit vor allem ein gemeinsames Verständnis des Begriffs der internationalen Übermittlung geschaffen werden.

Die CEH-Arbeitsgruppe *(CEH Expert Subgroup),* eine Kurzbezeichnung für Compliance, E-Government und Health, befasst sich mit Themen im Zusammenhang mit Zertifizierung und Akkreditierung sowie E-Government und Gesundheit. Betreffend Zertifizierung und Akkreditierung prüfte die CEH-Arbeitsgruppe in ihren Sitzungen im Berichtsjahr die Akkreditierungskriterien für Überwachungsstellen nach Art. 41 DSGVO und die Akkreditierungskriterien für Zertifizierungsstellen nach Art. 43 DSGVO von verschiedenen Mitgliedstaaten, zu denen der EDSA nachfolgend eine Stellungnahme verfassen sollte. Im Gesundheitsbereich als zweiter grosser Bereich der CEH-Arbeitsgruppe bildeten auch im Berichtsjahr COVID-19-bezogene Themen Teil des Arbeitsprogramms der CEH-Arbeitsgruppe. Die CEH-Arbeitsgruppe brachte hier ihre Expertise zu datenschutzrechtlichen Aspekten im Zusammenhang mit dem «Grünen Pass» ein. Ebenfalls explorierte die CEH-Arbeitsgruppe die datenschutzrechtlichen Implikationen aus der Forderung des U.S. Centers for Disease Control and Prevention (CDC), wonach Fluggesellschaften von ihren Fluggästen bei Flügen von Europa in die Vereinigten Staaten von Amerika den COVID-Status unter Vorlage entsprechender beweisender Dokumente zu erheben hatten. Datenschutzrechtlich standen bei letzterem insbesondere die Frage der Rechtsgrundlage für die diesbezügliche Verarbeitung der personenbezogenen Daten, und von Gesundheitsdaten im Speziellen, im Vordergrund ebenso wie die Aufbewahrungsdauer der erhobenen Daten und Dokumente. Teil der Aktivitäten der CEH-Arbeitsgruppe war im Berichtsjahr schliesslich auch die Analyse datenschutzrechtlicher Fragen zu Regelungsinstrumenten auf europäischer Ebene, so beispielsweise der Digital Governance Act (DGA). Der DGA soll eine gesetzliche Grundlage für die Weiterverwendung von bestimmten Daten, welche im Besitz von öffentlichen Stellen sind, ermöglichen. Auch der Digital Services Act (DSA) sei genannt. Dabei handelt es sich um eine Verordnung über digitale Dienste, die zum Ziele hat, a) den besseren Schutz von Verbraucherinnen und Verbrauchern im Internet zu garantieren, b) einen stringenten Rechenschaftsrahmen und eindeutige Transparenzregeln für Online-Plattformen zu schaffen und c) die Innovation, Entwicklung und Wettbewerbsfähigkeit im Binnenmarkt zu fördern.

Die Arbeitsgruppe zu technologischen Themen *(Technology Expert Subgroup)* befasste sich im Jahr 2021 mit einem breiten Spektrum an Fragestellungen und veröffentlichte einige Leitlinien, Empfehlungen sowie Stellungnahmen. An dieser Stelle seien beispielhaft die Leitlinien zu virtuellen Sprachassistenten wie auch die gemeinsame Stellungnahme mit der europäischen Datenschutzaufsichtsbehörde (EDPS) zur geplanten Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Artificial Intelligence Act) erwähnt. Weitere Leitlinien befinden sich derzeit in der Ausarbeitung. Insbesondere die Überarbeitung der Leitlinie zur Anonymisierung und Pseudonymisierung als auch die neue Leitlinie zum Thema Blockchain werden mit grossem Interesse erwartet. Derzeit werden in der Arbeitsgruppe weitere zukünftige Themen evaluiert. Um eine möglichst hohe Qualität der Dokumente gewährleisten zu können, steht die Arbeitsgruppe in einem ständigen Informationsaustausch mit relevanten Organisationen und Behörden, wie beispielsweise der Agentur der Europäischen Union für Cybersicherheit (ENISA).

Die Arbeitsgruppe zu Sozialen Medien *(Social Media Subgroup)* hat Empfehlungen zum Thema Benutzerschnittstellen-Design bei Plattformen Sozialer Medien ausgearbeitet. Diese Leitlinien sollen praktische Empfehlungen für Designer und Nutzer von Social-Media-Plattformen dafür bieten, wie sogenannte „Dark Patterns" in Social-Media-Schnittstellen, die gegen die DSGVO verstossen, bewertet und vermieden werden können. Die Arbeitsgruppe geht davon aus, dass die Empfehlungen nach der bis Mai 2022 dauernden öffentlichen Konsultation durch das Plenum verabschiedet werden. Des Weiteren sind Leitlinien für die Nutzung Sozialer Medien durch öffentliche Einrichtungen in Ausarbeitung. Das Dokument befindet sich noch in einem frühen Stadium, sodass mit einer Verabschiedung durch das Plenum erst gegen Ende 2022 zu rechnen ist.

Die BTLE-Arbeitsgruppe *(BTLE Expert Subgroup*), eine Kurzbezeichnung für Border Travel und Law Enforcement, hat sich im Berichtsjahr zu zehn (Online-) Sitzungen getroffen und befasste sich unter anderem mit einer Erklärung zum neuen Entwurf des zweiten Zusatzprotokolls zum Budapester Übereinkommen (Übereinkommen über Computerkriminalität). Zudem

wurde im Berichtsjahr die EDSA-Stellungnahme zur Angemessenheit des Datenschutzrechts des Vereinigten Königreichs (Angemessenheitsbeschluss) in Bezug auf die DSGVO sowie die Polizei-Richtlinie (EU) 2016 / 680 (LED) verabschiedet und Empfehlungen zu Art. 36 der LED (Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses) angenommen. Des Weiteren wurde von der Arbeitsgruppe die endgültige Version der Empfehlungen zu ergänzenden Massnahmen für Instrumente zum internationalen Datentransfer ausgearbeitet. Die Arbeitsgruppe hat zudem ein Antwortschreiben einer Europaabgeordneten zum automatischen Bilderkennungssystem für Migranten in Italien verfasst sowie die Stellungnahme des EDSA zum Entwurf eines Angemessenheitsbeschlusses der EU-Kommission zu Südkorea vorbereitet. Im Weiteren hat die Arbeitsgruppe den EDSA-Beitrag zur LED-Evaluierung erarbeitet und formell an die EU-Kommission übermittelt sowie eine EDSA-Antwort zu einem Schreiben eines Europaabgeordneten in Bezug auf einen angeblichen Einsatz von Spähsoftware durch öffentliche Behörden in Ungarn (Pegasus-Affäre) verfasst.

Das *DPO-Network* ist das Netzwerk der für die europäischen Datenschutz-Aufsichtsbehörden amtierenden Datenschutzbeauftragten. Ziel dieses Netzwerkes ist die Bildung von gemeinsamem 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.

7.1.2 Gegenseitige Amtshilfe

Wie eingangs erwähnt, erfordert die DSGVO nicht nur eine Zusammenarbeit der europäischen Datenschutz-Aufsichtsbehörden im bzw. mit dem EDSA, sondern auch eine intensive Kommunikation zwischen den einzelnen Aufsichtsbehörden, indem diese gemäss Art. 57 Abs. 1 Bst. g DSGVO «mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten». Die DSS erhielt im Berichtsjahr 75 Anfragen von anderen europäischen Datenschutzaufsichtsbehörden, was im Vergleich zu den im Vorjahr beantworteten 41 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 zum Löschen von gesammelten Daten bei Unterschriftensammlungen, Zutrittskontrollen im Zusammenhang mit Covid-19, Speicherung von biometrischen Daten, Datenaustausch mit einem Drittstaat, investigativen Journalismus mit Drohnen, Videoüberwachung, oder auch die automatische Nummernerkennung oder mobilitätsbezogene Anwendung von personenbezogenen Daten durch vernetzte Fahrzeuge.

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 2021 an der 41. und 42. Versammlung des Beratenden Ausschusses des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) des Europarats teilgenommen. Beide Veranstaltungen wurden auch in diesem Jahr nur digital per Videokonferenz durchgeführt.

Der Beratende Ausschuss der Konvention 108 hat sich im Berichtsjahr wieder intensiv mit datenschutzrechtlichen Fragen in der Pandemie befasst und eine Stellungnahme zu «Covid-19 vaccination, attestations and data protection» verfasst. Daneben hat er aber auch Leitlinien zu «Facial Recognition» und «on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns» verabschiedet. Im Übrigen bestand die Hauptarbeit des Beratenden Ausschusses weiterhin in der Erarbeitung von Berichten, Positionspapieren u.ä. zu den Themen Digitale Identitäten, zwischenstaatlicher Informationsaustausch zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung sowie zu Steuerzwecken, Standardvertragsklauseln für grenzüberschreitende Datentransfers, Datenschutz in politischen Kampagnen und Wahlen, sowie grenzüberschreitender Zugang zu Daten in der Strafverfolgung. Die Ergebnisse dieser Arbeiten können zu künftigen Handlungsempfehlungen, Leitfäden, Resolutionen oder Erklärungen auch übergeordneter Organe des Europarates führen. So hat etwa der Ministerrat im November 2021 eine Erklärung «on the need to protect children's privacy in the digital environment» sowie eine Empfehlung «on the protection of individuals with regard to automatic processing of personal data in the context of profiling» verabschiedet.

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 war die DSS weiter massgeblich in die Vorbereitung des Berichts und Antrags an den Landtag involviert. Die formelle Ratifikation des Änderungsprotokolls durch Liechtenstein wird für 2022 erwartet.

Des Weiteren hat die DSS das Amt für Auswärtige Angelegenheiten im Berichtsjahr bei der Beantwortung eines Fragebogens des Ad hoc Committee on Artificial Intelligence (CAHAI) des Europarats unterstützt, welches eine Multi-Stakeholder-Befragung zum Thema künstliche Intelligenz durchführte. Damit wollte das CAHAI – in Hinblick auf die mögliche Schaffung eines verbindlichen Rechtsrahmens – von öffentlichen wie auch privaten Akteuren Informationen für eine Machbarkeitsstudie wie auch zu regulatorischen Optionen im Bereich der künstlichen Intelligenz sammeln.

«Datenschutz ist kein Selbstzweck, sondern er ist ein Recht der Bürgerinnen und Bürger, das respektiert und geschützt werden muss.»

8. Schlussbemerkung und Ausblick

Wie bereits im Tätigkeitsbericht 2020 befürchtet, brachte das Berichtsjahr 2021 bedauerlicherweise keine Rückkehr zum ursprünglichen Arbeitsablauf in der DSS. Der Unterschied zum Vorjahr war lediglich, dass man zumindest im Grundsatz darauf eingestellt war und bereits auf ein Repertoire an alternativen Arbeitsmethoden zurückgreifen konnte. Der mehrfache Wechsel von der Anwesenheit im Büro in das Home-Office und zurück funktionierte problemlos, digitale Kanäle verhinderten Kommunikations- und Informationslücken und die fast lückenlose Teilnahme an den online stattfindenden Sitzungen des EDSA konnte gesichert werden. All dies war zur neuen Normalität geworden und sicherte einen reibungslosen Ablauf der unterschiedlichen Tätigkeiten der DSS.

Der Verzicht der DSS auf amtswegige Datenschutzüberprüfungen bei Unternehmen mag zwar zur Erleichterung bei Letzteren geführt haben, bedeutet aber aus Sicht der DSS einen gewissen Rückschritt bzw. Stagnation des Fortschritts in Bezug auf die Umsetzung der Datenschutzvorschriften bei jenen Unternehmen, die diesbezüglich nach wie vor grosse Lücken aufweisen. Die DSS sieht es gerade angesichts der zunehmenden Zahl an Meldungen von Datenschutzpannen gemäss Art. 33 DSGVO sowie der Beschwerden, die vielfach grundlegende Pflichten der Verantwortlichen zum Gegenstand haben, als unumgänglich, 2022 erneut amtswegige Prüfungen durchzuführen.

Wenn somit der Rückblick auf das Berichtsjahr aus Sicht der DSS durchwegs positiv ausfällt, darf man nicht die Augen davor verschliessen, dass Datenschutz in der öffentlichen Wahrnehmung nach wie vor mancherorts als Belastung oder gar als Einschränkung der persönlichen Freiheiten, wie etwa der Meinungsfreiheit, verstanden wird. Diese kritischen Stimmen sind ernst zu nehmen und das Gespräch zu suchen. Der gute Zweck einer Datenverarbeitung rechtfertigt es nicht, auf die Einhaltung des Datenschutzes zu verzichten. Und so kann es auch keine umfassende Erlaubnis zur Derogation von datenschutzrechtlichen Bestimmungen geben. Wenngleich die DSS nach Möglichkeit bemüht ist, den bürokratischen Aufwand für die Umsetzung des Datenschutzes in Grenzen zu halten und machbare Lösungen zu propagieren, so darf dies nie dazu führen, dass dieser Einbussen erleiden muss. Datenschutz ist kein Selbstzweck, sondern er ist ein Recht der Bürgerinnen und Bürger, das respektiert und geschützt werden muss.

Ein Ausblick auf das Jahr 2022 lässt vorsichtigen Optimismus aufkommen. Im Vergleich zum vergangenen Jahr scheint dieser Optimismus diesmal doch angebracht, die «neue Normalität» zumindest zu einem Teil wieder durch die «alte Normalität» zu ersetzen. So sollte der Datenschutztag, der ursprünglich im Januar 2021 und dann im Januar 2022 hätte stattfinden sollen, am 2. Juni 2022 tatsächlich Wirklichkeit werden.

Datenschutzstelle Fürstentum Liechtenstein
Städtle 38
Postfach 684
FL-9490 Vaduz

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