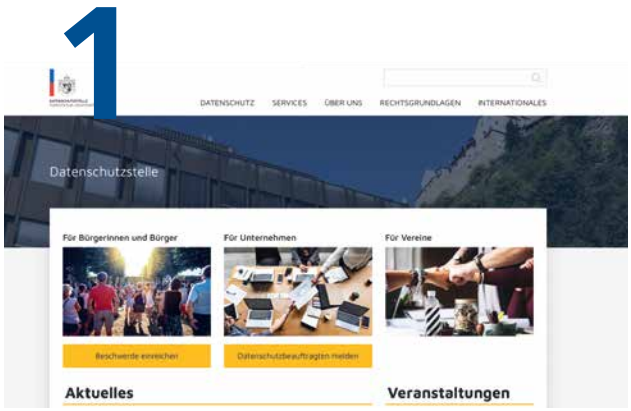
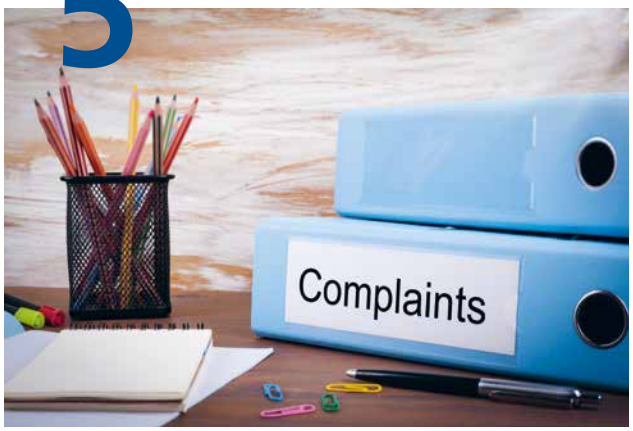
DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht Datenschutzstelle
Fürstentum Liechtenstein

Tätigkeitsbericht 2019

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

Im Tätigkeitsbericht 2018 begann das Kapitel zur Internationalen Zusammenarbeit mit der folgenden Feststellung: «*Mit der Datenschutz-Grundverordnung (DSGVO) wurde die bisherige Rolle der Datenschutzstelle als ein autonomer, nationaler Akteur in einem nationalen Umfeld mit nur wenigen Berührungspunkten nach aussen abgelöst. Künftig muss sich die Datenschutzstelle – wie auch alle anderen europäischen Datenschutzaufsichtsbehörden – als Teil eines europäischen Projekts sehen, denn nur so kann der in der Grundverordnung geforderte harmonisierte Ansatz erreicht und auf einheitliche Rechte und Pflichten im EWR hingewirkt werden.*»

Zum damaligen Zeitpunkt war dies als Szenario für die weitere Zukunft gedacht, heute ist der Moment gekommen, diese Intention auf seine Realisierung im Berichtsjahr zu überprüfen. Der erste Teil der Antwort fällt eindeutig aus, der Blick der Datenschutzstelle nach Europa war im Bereich Datenschutz wohl noch nie so häufig wie im Berichtsjahr. Das europäische Ausland und seine Aufsichtsbehörden, aber auch Gerichte warteten mit einer Vielzahl von Entscheidungen auf, die auch Geldbussen in beträchtlicher Höhe umfassten. Die Informationen und Stellungnahmen der Aufsichtsbehörden zu unterschiedlichen Themenbereichen, Kommentare der Wissenschaft und Lehre sowie die Richtlinien und Empfehlungen des Europäischen Datenschutzausschusses wollten berücksichtigt werden. Dazu kamen die im Berichtsjahr nicht ausgebliebenen Skandale und Schlagzeilen rund um soziale Medien, neue technische Entwicklungen in- und ausserhalb Europas, teils kontroverse Debatten um Fragen zu Dateneigentum, Cyber-Sicherheit, Cookies, Einsatz von Social-Plugins oder Datenschutz im Wandel der Mobilität. Vieles davon betraf Liechtenstein nicht direkt oder nur marginal. Dennoch wollten all diese Entwicklungen beobachtet und gewürdigt werden und konnten aus der Arbeit der Datenschutzstelle nicht ausgeklammert werden.

Der zweite Teil der Antwort betrifft die Autonomie der Datenschutzstelle in Bezug auf Europa. Auch wenn die Datenschutzstelle im Vergleich zur Zeit vor der Geltung der DSGVO nicht mehr als völlig autonomer Akteur betrachtet werden kann, so zeigt das Berichtsjahr, dass den Aufsichtsbehörden nach wie vor ein bedeutender Spielraum bleibt, in dem sie agieren und ihre Entscheidungen treffen können. Die Datenschutzstelle nutzte diesen Spielraum, indem sie zwar die europäischen Entwicklungen genau beobachtete, sie aber nicht ungeprüft übernahm, sondern soweit möglich auf die Verhältnisse in Lichtenstein anpasste.

Dr. Marie-Louise Gächter, Leiterin Datenschutzstelle

Vaduz, im April 2020

Einleitung

Der Begriff *Zwischenbilanz* war im Berichtsjahr in Bezug auf die Umsetzung der DSGVO allgegenwärtig und stand häufig im Mittelpunkt der medialen Berichterstattung sowie der unzähligen Veranstaltungen zum Thema Datenschutz. Auch dieser Tätigkeitsbericht ist eine Art Zwischenbilanz. Die bedeutendste Erkenntnis ist dabei, dass sich die Umsetzung der Datenschutzbestimmungen nach wie vor in der Lernphase bzw. optimistisch gesehen in der Konsolidierungsphase befindet.

Der Rückblick auf die Umsetzung in Liechtenstein im Berichtsjahr lässt sich vereinfacht mit dem in Europa gerne, wenngleich in anderem Kontext zitierten Bild der zwei Geschwindigkeiten zusammenfassen. In Bezug auf den Datenschutz und die Erfahrungen der Datenschutzstelle will dies heissen, dass wir als Aufsichtsbehörde zum einen positiv feststellen konnten, dass eine grosse Zahl der Verantwortlichen dem Datenschutz einen bedeutenden Stellenwert in ihrem Unternehmen oder ihrer Institution eingeräumt hat und diesen Stellenwert in Kooperation mit der Datenschutzstelle weiter ausbauen konnte. Erfreulich war hier auch die Rückmeldung, dass diese Institutionen mit ihrer Entscheidung, dem Datenschutz den ihm gebotenen Platz einzuräumen, viel positive Resonanz bei Kunden, Mitarbeitenden oder anderen betroffenen Personen erzielen konnten und somit der Datenschutz für sie tatsächlich einen Mehrwert brachte.

Auf der anderen Seite der Waagschale fanden sich jene Institutionen, die den richtigen Moment der Umsetzung verpasst haben und darauf bauten, dass es wohl nicht auffiele, wenn sie den Datenschutz nicht in ihre Unternehmensstrategie aufnähmen oder ihm nur eine unbedeutende Nebenrolle zuschrieben. Es fiel und fällt allerdings sehr wohl auf und wir machten im Berichtsjahr von unseren Befugnissen weitreichend Gebrauch, um dem Datenschutz jene Rolle zukommen zu lassen, welche die DSGVO und das nationale Datenschutzgesetz für ihn vorgesehen hat.

Nichtsdestotrotz stand auch im Berichtsjahr die Beratung im Mittelpunkt der Tätigkeiten der Datenschutzstelle. Im Vergleich zum Vorjahr allerdings stellten die Beratungsanfragen das Team der Datenschutzstelle vor echte Herausforderungen, denn die Anfragen zeichneten sich durch eine merklich zunehmende Komplexität aus und nahmen wesentlich mehr Zeit in Anspruch. Die Zwischenbilanz, die wir am Ende des Berichtsjahrs ziehen konnten, bestätigte aber einmal mehr, dass der 2018 lancierte kommunikative Ansatz erneut der richtige war, vor allem in einem Land, wo die Wege der Verantwortlichen und Auftragsverarbeiter zur Aufsichtsbehörde kurz und unbürokratisch sind.

Durch die Kommunikation mit den Verantwortlichen und Auftragsverarbeitern sowie betroffenen Personen und anderen am Datenschutz Interessierten konnten auch wir sehr viel lernen und ihre Bedürfnisse, Schwierigkeiten und Erfahrungen mit dem Thema Datenschutz vertieft kennenlernen. Und damit bestätigte sich in der Zwischenbilanz eine zweite Feststellung, die wir 2018 getroffen haben: Datenschutz ist immer ein Gemeinschaftsprojekt und darf nicht gleichgesetzt werden mit der Durchsetzung von Rechtsbestimmungen von oben nach unten. Wir bedanken uns bei allen, die zum Gelingen des Gemeinschaftsprojektes im Berichtsjahr beigetragen haben, wissen aber, dass es nach wie vor viel Überzeugungsarbeit brauchen wird, um die zwei Geschwindigkeiten aneinander anzugleichen und tatsächlich zu einer einheitlichen und konsequenten Umsetzung des Datenschutzes in Liechtenstein zu gelangen.

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

1. Öffentlichkeitsarbeit

Die Öffentlichkeitsarbeit nimmt einen zentralen Stellenwert in der Informationsvermittlung im Bereich Datenschutz ein. Informationen und allgemeingültige datenschutzrechtliche Positionen der Aufsichtsbehörde, aber auch weiterer Akteure wie des Europäischen Datenschutzausschusses, anderer europäischer Aufsichtsbehörden oder nationaler und europäischer Gerichte sollen allgemein bekannt und sowohl für Verantwortliche und Auftragsverarbeiter als auch für betroffene Personen zugänglich gemacht werden.

Für die Vermittlung von Fachinformationen nutzt die Datenschutzstelle vor allem vier Kanäle: Veranstaltungen und Vorträge, Newsletter, ihre Internetseite und individuelle Beratungen. Insbesondere das Zusammenwirken der genannten Kommunikationskanäle ermöglicht es, dass eine sehr grosse Zahl an Adressaten erreicht werden kann. Einen bedeutenden Mehrwert brachte im Berichtsjahr wieder die erfolgreiche und konstruktive Zusammenarbeit mit Verbänden, Gemeinden, Medien und Universitäten. Neu umfasste die Informationsvermittlung das Datenschutzgesetz, die Datenschutzverordnung, die Datenschutzbestimmungen in den Spezialgesetzen sowie im kommunalen Bereich die Verordnung über die Offenlegung bestimmter personenbezogener Daten durch die Gemeinden, welche allesamt am 1. Januar 2019 in Kraft getreten sind.

1.1 Veranstaltungen

Die Datenschutzstelle organisierte im Berichtsjahr zwei Veranstaltungen in Eigenverantwortung. Der *Datenschutztag* am 29. Januar im Vaduzer Saal widmete sich dem Thema «Meine Daten gehören mir! – Jetzt erst ‹Recht›!» Gastreferent Dr. Christof Tschohl, wissenschaftlicher Leiter und Miteigentümer des Forschungs- und Beratungsunternehmens Research Institute – Digital Human Rights Center, erläuterte den 250 Besuchern ihre Rechte und zeigte auf, wie sie ihre Schutzmöglichkeiten erkennen und wahrnehmen können. Im Anschluss diskutierten Experten aus Technik und Wirtschaft, wie die Rechte der Betroffenen – aus Sicht der Verbraucher und der Unternehmen in Liechtenstein – gewahrt und umgesetzt werden können. Nach Ende der Veranstaltung lud die Datenschutzstelle zu einem Networking-Apéro ein.

Während das Zielpublikum am Datenschutztag die breite Öffentlichkeit war, richtete sich das *Vernetzungstreffen* am 7. November an die Fachexperten, sprich die betrieblichen Datenschutzbeauftragten. Ziel war es, diese über die aktuelle Arbeit und die Tätigkeitsschwerpunkte der Datenschutzstelle im Berichtsjahr zu informieren und über neueste Grundsatzentscheide im In- und Ausland in Kenntnis zu setzen. Darüber hinaus wurde ihnen Gelegenheit gegeben, Fragen zu stellen und Kernbereiche ihrer täglichen Arbeit zu diskutieren sowie sich untereinander zu vernetzen.

1.2 Vorträge

1.2.1 Schwerpunkt Schulung Gemeinden

Gespräche zu Beginn des Berichtsjahres mit einzelnen Gemeinden zeigten, dass die Gemeinden Unterstützung bei der Ausbildung ihrer Mitarbeitenden in der datenschutzrechtlichen Bewertung von Sachverhalten wünschten. Wenngleich die Gemeinden durch einen externen Datenschutzbeauftragten gut beraten werden, erschien es ihnen wichtig, den Mitarbeitenden eine klare und gut verständliche Orientierung aus Sicht der Datenschutz-Aufsichtsbehörde zu vermitteln. Aus diesem Grund bot die Datenschutzstelle an, Schulungen für sämtliche Mitarbeitende in den elf Gemeinden durchzuführen, bestehend aus einem rechtlichen sowie einem technischen Teil. Zusätzlich konnten die Gemeinden der Datenschutzstelle im Vorfeld oder im Nachgang der Schulung spezifische Fragen zukommen lassen. Sowohl die Schulungsveranstaltungen als auch die Möglichkeit, weitere Fragen zu stellen, wurden von den Gemeinden rege genutzt. Unter den am häufigsten gestellten Fragen fanden sich die Folgenden:

Kann sich eine Gemeinde auf die Rechtsgrundlage der berechtigten Interessen in Art. 6 Abs. 1 Bst. f DSGVO stützen?

Gemäss Art. 6 Abs. 1 Unterabsatz 2 DSGVO ist Art. 6 Abs. 1 Bst. f DSGVO nicht für die von Behörden in Erfüllung ihrer gesetzlich definierten Aufgaben vorgenommenen Datenverarbeitung anwendbar. Gemeint sind an dieser Stelle sowohl die Pflicht als auch die freiwilligen Aufgaben, die eine Gemeinde erfüllt. Dies gilt allerdings nicht, wenn die Behörde in gleicher Weise wie private Akteure am Privatrechtsverkehr teilnimmt, wenn sie etwa als Arbeitgeberin oder Vermieterin von Immobilien auftritt oder einen Werkvertrag abschliesst. In diesen Bereichen bieten die berechtigten Interessen auch für die Gemeinden eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten.

Gelten Daten Verstorbener als personenbezogene Daten?
Grundsätzlich gelten personenbezogene Daten Verstorbener gemäss Erwägungsgrund 27 nicht als Daten im Sinne der DSGVO. Allerdings können bestimmte Daten eines Verstorbenen einen Bezug zu einer lebenden Person haben und insoweit Personenbezug aufweisen (z. B. Informationen bezüglich des Vorliegens einer Erbkrankheit beim Verstorbenen, welche Rückschlüsse auf den Gesundheitszustand der Nachkommen zulassen).

Dürfen anlässlich einer öffentlichen Veranstaltung der Gemeinde Fotos gemacht und danach veröffentlicht werden bzw. bedarf es in jedem Fall einer Einwilligung der abgebildeten Personen?
Die Veröffentlichung von Berichten und Bildern über Veranstaltungen ist keine hoheitliche Aufgabe und kann daher eine Rechtfertigung in den berechtigten Interessen der Gemeinde gemäss Art. 6 Abs. 1 Bst. f DSGVO finden. Bei der Abwägung der Gemeindeinteressen mit den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person ist vor allem zwischen Übersichtsaufnahmen und der Aufnahme einzelner Personen zu unterscheiden. Während erstere im Regelfall von den berechtigten Interessen der Gemeinde gedeckt sind, muss im zweiten Fall, in dem einzelne Personen hervorgehoben auf den Fotos erkennbar sind, grundsätzlich deren Einwilligung eingeholt werden. Bei Personen von öffentlichem Interesse wie z. B. Gemeinderäten ist keine Einwilligung einzuholen. Hingegen bedarf es einer Einwilligung, wenn es sich um Abbildungen von Kindern handelt. Zudem hat die Gemeinde – unabhängig von der gewählten Rechtsgrundlage – die Informationspflicht gemäss Art. 13 DSGVO zu beachten.

Ist die Gemeinde die verantwortliche Stelle für Datenverarbeitungen durch den Gemeinderat bzw. Mitglieder des Gemeinderates?
Die datenschutzrechtliche Verantwortung einer Gemeinde umfasst auch die Tätigkeit ihres Gemeinderats und die Verarbeitung personenbezogener Daten durch Mitglieder des Gemeinderats. So ist die verantwortliche Stelle die Gemeinde vertreten durch den Gemeindevorsteher.

Dürfen Unterlagen von öffentlichen Gemeinderatssitzungen im Internet veröffentlicht werden?
Grundsätzlich ist von der Gemeinde sicherzustellen, dass keine personenbezogenen Daten unbefugt offengelegt werden. Der Grundsatz der Öffentlichkeit der Sitzungen ist nicht automatisch eine geeignete Rechtsgrundlage, personenbezogene Daten etwa in Protokollen im Internet zu veröffentlichen. Insbesondere ist abzuwägen, ob die jeweilige Nennung personenbezogener Daten tatsächlich erforderlich ist oder ob eine Information der Öffentlichkeit etwa ohne explizite Nennung eines Namens etc. erreicht werden kann.

Ist die Einbindung von Plug-ins Sozialer Netzwerke in die Internetseite der Gemeinde zulässig?
Die Frage ist grundsätzlich zu verneinen. Ist ein Besucher der Internetseite der Gemeinde gleichzeitig im Sozialen Netzwerk des Plug-in-Herstellers angemeldet, wird er von letzterem identifiziert und das Nutzungsverhalten auf der Internetseite der Gemeinde wird seinem Profil zugeordnet. Der Plug-in-Hersteller kann somit nachvollziehen, wer wann welche Informationen auf der Internetseite der Gemeinde abgerufen hat. Aufgrund der Einbindung erhält die hinter dem Plug-in stehende Institution (Soziales Netzwerk) allein durch den Aufruf der Internetseite der Gemeinde als Information zumindest die IP-Adresse des Besuchers. Da für diesen Datenfluss die Rechtsgrundlage fehlt (ausser die Gemeinde hat dafür eine Einwilligung eingeholt), ist die Einbindung in die Internetseite der Gemeinde nicht zulässig.

Auf welcher Rechtsgrundlage darf die Gemeinde Daten an Dritte weitergeben?
Neben den Bestimmungen in Spezialgesetzen findet sich eine entsprechende allgemeine Rechtsgrundlage in der Verordnung vom 11. Dezember 2018 über die Offenlegung bestimmter personenbezogener Daten durch die Gemeinden. Diese Verordnung erlaubt es den Gemeinden, auf schriftliche Anfrage und bei Vorliegen bestimmter Voraussetzungen Dritten bestimmte personenbezogene Daten offenzulegen. Eine der Voraussetzungen ist die Abwägung der berechtigten Interessen des anfragenden Dritten mit den schutzwürdigen Interessen der betroffenen Person am Ausschluss der Offenlegung. Dies hat zwar für jeden Einzelfall gesondert zu erfolgen, sollte jedoch in der künftigen Praxis zu einer einheitlichen Auslegung und Anwendung durch die Gemeinden führen. Die Datenschutzstelle regte deshalb bei den Gemeinden einen Austausch über ihre jeweilige Praxis an mit dem Ziel, die Einheitlichkeit der Anwendung dieser Verordnung auch gemeindeüberschreitend zu erreichen.

1.2.2 Schwerpunkt Kinder und Datenschutz

Die Notwendigkeit des besonderen Schutzes von Kindern wird in Erwägungsgrund 38 der DSGVO klar zum Ausdruck gebracht:

«*Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen.*»

Dieser Notwendigkeit eines besonderen Schutzes von Kindern wurde von der Datenschutzstelle im Berichtsjahr mehrfach Rechnung getragen.

Im Mai 2019 erhielt die Datenschutzstelle eine Anfrage von der Fachgruppe Medienkompetenz hinsichtlich zweier gemeinsamer *Veranstaltungen für die Oberstufe der Waldorfschule in Schaan*. Das Ziel der ersten Sensibilisierungsveranstaltung mit ca. vierzig Jugendlichen war es, während des halbtägigen Workshops die Medienkompetenz der Schülerinnen und Schüler zu fördern sowie ihnen datenschutzrelevante Aspekte näherzubringen. Die Jugendlichen waren sehr wissbegierig, motiviert und zum Teil sehr gut über die Chancen und Risiken im Umgang mit digitalen Medien informiert. Während des Workshops wurden vier Gruppen gebildet, innerhalb derer sich die Jugendlichen über vorgegebene Themenbereiche wie Gaming, WhatsApp etc. austauschten und Antworten auf gestellte Fragen ausarbeiten mussten. Nach der Gruppenarbeit stellte eine Person pro Gruppe die Erkenntnisse im Plenum vor.

Der zweite Termin wurde im Rahmen eines Elternabends organisiert. Auf Wunsch der Schule und aufgrund der Rückmeldungen von Eltern wurden neben Persönlichkeitsrechten wie zum Beispiel dem Recht am eigenen Bild auch Themen wie Sexting, Cyber-Mobbing, Sicherheit von Passwörtern und Möglichkeiten zum Schutz der Privatsphäre im digitalen Zeitalter erörtert. Die Veranstaltung mit den Eltern der Jugendlichen war ebenfalls interaktiv gestaltet. Als Diskussionsbasis dienten die Erfahrungen und Resultate aus dem Workshop mit den Jugendlichen. Während den Gesprächen zeigten die Eltern Besorgnis im Hinblick auf die Gesellschaft im Allgemeinen und die Nutzung von Smart Devices im Speziellen.

Auf Anfrage des Haus Gutenberg in Balzers wurde von der Datenschutzstelle in Kooperation mit der Fachgruppe Medienkompetenz im Herbst 2019 eine zweite *Sensibilisierungsveranstaltung, bestehend aus zwei Seminaren zum Thema «Mein Kind will ein Smartphone»*, lanciert. Die erste Veranstaltung fand im September unter dem Titel «Mein Kind will ein Smartphone – darauf sollten Eltern achten» statt. In diesem Kurs wurde dargelegt, auf welche Aspekte Eltern bei ihren Kindern hinsichtlich der Nutzung von Smartphones achten sollten und wie die Eltern sie dabei optimal unterstützen können. Es wurden wertvolle Hinweise zu altersrelevanten Fragestellungen und Verhaltensweisen im Zusammenhang mit der Nutzung digitaler Medien gegeben. Aufgrund der Ausführungen zeigte sich deutlich, dass Altersempfehlungen bei Kindern zur Nutzung von digitalen Medien sehr stark von der Entwicklung und vom Umfeld eines Kindes abhängen und somit aufgrund der Nähe die Eltern ihre Kinder im Umgang mit digitalen Medien am optimalsten begleiten können. Des Weiteren wurden bei Kindern beliebte Spiele-Apps aus Sicht des Datenschutzes näher beleuchtet. Ziel war es, konkrete Tipps zu Einstellungsmöglichkeiten zu geben und Verhaltensweisen aufzuzeigen, sodass die Privatsphäre der Kinder im Umfang mit dem Smartphone soweit als möglich gewahrt werden kann.

Das zweite Seminar, welches in Form eines Workshops unter demselben Titel «Mein Kind hat ein Smartphone – darauf sollten Eltern achten» durchgeführt wurde, hatte den Fokus, den Eltern gemeinsam mit ihren Kindern praxisbezogenes Wissen zum Thema Datenschutz sowie Massnahmen zur «digitalen» Suchtprävention zu vermitteln. Dazu waren die Teilnehmerinnen und Teilnehmer angehalten, ihre eigenen Smartphones mitzubringen. Gemeinsam wurden die Einstellungen zum Schutz der Privatsphäre besprochen, überprüft und Fragen dazu beantwortet. Neben den konkreten Einstellungsmöglichkeiten in bei Kindern und Jugendlichen beliebten Apps wurden die zwei meist verwendeten Betriebssysteme auf Smartphones, Android und iOS, näher betrachtet.

Eine dritte Sensibilisierungsveranstaltung fand auf *Einladung der LGT Bank für etwa zwanzig Lernende im ersten und zweiten Lehrjahr* statt. Eingeleitet wurde der Kurs mit dem Titel «Datenschutz in Sozialen Netzwerken – Ein Blick hinter die Kulissen» mit einem historischen Abriss von der Entstehung und Entwicklung des Internets im Kontext des Datenschutzes. Die theoretische Einführung des Themas wurde durch Fragestellungen wie zum Beispiel «Wer sammelt meine Daten und wer liest mit? Warum ausspionieren? Wen interessiert's?" abgerundet. Auf Basis der vermittelten Hintergrundinformationen wurden die Lernenden anschliessend aufgerufen, in einer Gruppenarbeit Argumente, die für oder gegen den Datenschutz sprechen, auszuarbeiten. Im Anschluss wurden die ausgearbeiteten Argumente der Pro und Contra Gruppen durch jeweils einen Vertreter bzw. eine Vertreterin der Gruppe vorgebracht und innerhalb des Plenums diskutiert. Die

Datenschutzstelle moderierte, gab Rückmeldungen und lieferte den Jugendlichen weitere Ideen und Denkanstösse.

1.2.3 Kooperation mit den Universitäten in Liechtenstein

Die bereits im Vorjahr erfolgreiche Zusammenarbeit mit den Universitäten in Liechtenstein konnte im Berichtsjahr noch intensiviert werden.

Im Mai und September fanden an der Universität Liechtenstein der vierte und fünfte Durchgang des zweitägigen *Intensivkurses für betriebliche Datenschutzbeauftragte* statt. Die Datenschutzstelle konnte dabei wieder den ersten Teil zu den Grundsätzen der Datenverarbeitung unter der DSGVO übernehmen und einen umfassenden Einblick in die praxisrelevanten Fragestellungen geben, die von der Datenschutzstelle seit Geltung der DSGVO behandelt wurden.

Neu übernahm die Datenschutzstelle im *Zertifikatsstudiengang Compliance-Officer* der Universität Liechtenstein im September 2019 einen Vorlesungsteil zum Datenschutz und zur Datensicherheit. Datenschutzbeauftragte und Compliance Officer nehmen unterschiedliche Rollen im Unternehmen ein und haben auch unterschiedliche Funktionen, Kompetenzen, Befugnisse und Zielsetzungen. Hauptaugenmerk eines Compliance Officers ist jeweils die Vermeidung von Haftungsrisiken des Unternehmens sowie eine positive Aussenwirkung durch nachweisbare Transparenz. Im Mittelpunkt des Datenschutzes stehen dagegen die betroffenen Personen und der Schutz ihrer personenbezogenen Daten. Aus diesem Grund stellen aus Sicht der Datenschutzstelle nicht nur ein professionelles, aufgabenübergreifendes Compliance Management System, sondern auch gut ausgebildete Mitarbeitende in beiden Bereichen wichtige Indikatoren für die Transparenz und Qualität eines Unternehmens dar.

An der Vortragsveranstaltung *«Internet und Recht»* am 28. Mai, welche der Propter Homines Lehrstuhl für Bank- und Finanzmarktrecht der Universität Liechtenstein in Kooperation mit der Datenschutzstelle veranstaltete, beteiligte sich die Datenschutzstelle mit zwei Referaten. Der erste Vortrag befasste sich mit dem Thema Datenschutz von Kindern bei der Nutzung von Sozialen Medien. Obwohl dem Schutz von Kindern in der DSGVO an mehrfacher Stelle besonderes Augenmerk geschenkt wird, ist in der Praxis nicht immer gesichert, dass sich die Verantwortlichen ausnahmslos an diese Vorgaben halten. Umso wichtiger ist es daher, dass Kinder frühzeitig lernen, sich vorsichtig und verantwortungsvoll in der digitalen Welt zu bewegen. Ebenso kommt den Eltern eine bedeutende Rolle zu, indem sie gefordert sind, hier unterstützend mitzuwirken. Der blosse Verlass auf die neuen Datenschutzbestimmungen genügt gerade bei Kindern nicht.

Der zweite Vortrag der Datenschutzstelle führte in die «digitale Backstube» und erläuterte den Begriff «Cookies» und deren Funktionsweise. Cookies sind nichts anderes als kleine Textdateien, deren datenschutzrechtliche Einordnung stets von ihrem Zweck abhängig zu machen ist. Während etwa «Session-Cookies» meist völlig unbedenklich sind – ja für den Besuch einer Internetseite sogar hilfreich oder gar notwendig sein können –, können sich bei «Drittanbieter-Cookies» durchaus datenschutzrechtliche Problemstellungen ergeben, sofern eine entsprechende Einwilligung der betroffenen Personen nicht vorliegt.

Die Veranstaltung am 10. April an der Privaten Universität im Fürstentum Liechtenstein zum Thema *«Kann die Vorratsdatenspeicherung in den Zeiten der DSGVO noch gerechtfertigt werden?»* widmete sich einem Thema, welches in der jüngeren Vergangenheit von der Diskussion rund um die DSGVO etwas verdrängt worden war. Seit 2011 hat der Europäische Gerichtshof (EuGH) in Luxemburg vor allem in den Rechtssachen *Digital Rights Ireland* im Jahr 2014 (C-293/12 und C-594/12) und *Tele 2* im Jahr 2016 (C-203/15 und C-698/15) klare Massstäbe dafür gesetzt. Referenten aus Deutschland, Österreich und Liechtenstein – vertreten durch die Datenschutzstelle – gingen der Frage nach, ob diese Massstäbe in den genannten Ländern berücksichtigt und umgesetzt worden sind. Während in Deutschland die Vorratsdatenspeicherung wegen des Abwartens eines weiteren Urteils des EuGH ausgesetzt wurde und in Österreich die «Vorratsdatenspeicherung Light» als Kompromiss eingesetzt wird, zeigt sich das liechtensteinische Gesetz über die elektronische Kommunikation (Kommunikationsgesetz; KomG) aus Sicht der Datenschutzstelle und mit Blick auf den Datenschutz nach wie vor (zu) grosszügig in Bezug auf die Vorratsdatenspeicherung, und es bleiben Zweifel, ob diese Rechtslage das Einverständnis des EuGH bzw. des EFTA-Gerichtshofes finden würde.

Am 17. Dezember fand ebenfalls in Kooperation mit der Privaten Universität im Fürstentum Liechtenstein eine eintägige Weiterbildungsveranstaltung zum Thema *«Zwischenbilanz zur DSGVO. Was hat sich mit der DSGVO verändert?»* statt. Die Veranstaltung hatte einen Austausch zwischen österreichischen, deutschen und liechtensteinischen Vertretern bzw. Vertreterinnen der Datenschutz-Aufsichtsbehörden sowie Vertretern von Unternehmern aus den drei Ländern zum Ziel. Auch hier war die Datenschutzstelle mit zwei Vorträgen vertreten. Im ersten Vortrag wurde die Tätigkeit der Datenschutzstelle sowie ihr Arbeitsan-

satz präsentiert. Das von ihr verfolgte kommunikative Konzept mit dem Schwerpunkt Beratung unterscheidet die Datenschutzstelle zum Beispiel klar von der österreichischen Behörde, die ihren Fokus vornehmlich auf den Vollzug ausrichtet. Die bayrische Behörde hingegen konzentriert sich bei ihrer Tätigkeit ebenfalls auf die Beratung, wenngleich diese nicht ganz so stark ausgeprägt ist wie bei der Datenschutzstelle.

Der zweite Vortrag befasste sich mit dem spezifischen Thema der gemeinsamen Verantwortlichkeit im Sinne des Art. 26 DSGVO. In der Auslegung und Anwendung dieses Artikels birgt vor allem die Rechtsprechung des EuGH einiges an Brisanz. Bislang hat der Gerichtshof in drei Fällen zur gemeinsamen Verantwortlichkeit Stellung bezogen, zuletzt am 29. Juli 2019 in der Rechtssache *Fashion ID GmbH & Co. KG gegen Verbraucherzentrale NRW e. V.* (C-40/17). Gemäss diesen Urteilen reicht eine Mitwirkung an der Entscheidung über die Zwecke und Mittel der Verarbeitung mit einem Mindestmass an Einfluss auf die Verarbeitung personenbezogener Daten selbst bereits aus, um als gemeinsam Verantwortlicher qualifiziert zu werden. Diese datenschutzfreundliche Auslegung des Gerichtshofs ist auch für Verantwortliche in Liechtenstein von grosser Bedeutung, etwa innerhalb eines Konzerns. Wenn Verantwortliche eine gemeinsame Verantwortung feststellen, hat dies Auswirkungen insbesondere auf das Verarbeitungsverzeichnis, die Vertragsgestaltung mit Dienstleistern und Partnern im Konzern sowie mit Aussenstehenden, die Betroffenenrechte, die Umsetzung von Sicherheitsmassnahmen sowie die Haftungsregelungen.

1.2.4 Weitere Vorträge

Zusätzlich nahmen Mitarbeitende der Datenschutzstelle im Berichtsjahr an weiteren 33 Informations- und Diskussionsveranstaltungen als Referentinnen bzw. Referenten teil oder hielten Vorträge an Weiterbildungsveranstaltungen. Beispiele waren Informationsveranstaltungen der Treuhandkammer, des Amtes für Umwelt, des Vereins unabhängiger Vermögensverwalter, des Roten Kreuzes, der Liechtenstein Digital oder von ProIT Liechtenstein. Bis auf die letzten beiden Vorträge ging es vornehmlich um die Umsetzung der DSGVO und des DSG in Liechtenstein sowie die Pflichten, die dafür von den Verantwortlichen und Auftragsverarbeitern erfüllt werden müssen.

Die vierte Ausgabe des Ligital-Events im Technopark Liechtenstein stand unter dem Titel *«Lass dich nicht vom Datenschutz eiskalt erwischen.»* Die Datenschutzstelle betonte bei dieser Veranstaltung in einem Referat, dass der Datenschutz jeden betrifft und sich die Verantwortlichen frühzeitig damit auseinandersetzen sollten, da das Thema sehr breit ist und zahlreiche Aspekte und Grundsätze berücksichtigt werden müssen. Da für viele Teilnehmende die Frage «Wo beginnen?» im Zentrum stand, wurde von der Datenschutzstelle vor allem darüber informiert, wie Unternehmen mit überschaubarem Aufwand die wichtigsten Verpflichtungen erfüllen können und was dabei jeweils zu beachten ist. Wesentlich ist, dass durch den Verantwortlichen jene Datenverarbeitungsvorgänge zuerst betrachtet werden, welche die grössten Risiken für die betroffenen Personen bergen.

Die vom Verband der IT-Profis in Liechtenstein (proIT) organisierte Vortragsveranstaltung am 24. September befasste sich mit *Cyber-Sicherheit*. Auch an dieser Veranstaltung war die Datenschutzstelle mit einem Referat vertreten. Die Auswirkungen der DSGVO auf die Folgen eines Cyberangriffs sind vielfach noch unbekannt bzw. werden ignoriert. Aufgrund der Vorgaben der DSGVO kann vor allem die Höhe der durch einen Cyberangriff verursachten Kosten eine gesteigerte Dimension erreichen. Wie aktuelle Fälle in der EU im Berichtsjahr aufgezeigt haben, können zu den Kosten für die Systemwiederherstellung und -verbesserung überdies Geldbussen unter der DSGVO hinzukommen, begründet durch eine Verletzung der Art. 5 Abs. 1 Bst. f und Art. 32 DSGVO. Art. 5 und 32 DSGVO fordern, dass personenbezogene Daten so verarbeitet werden, dass eine angemessene Sicherheit dieser Daten gewährleistet ist, einschliesslich des Schutzes vor dem Risiko der Zerstörung, des Verlusts, der Änderung und der unbefugten Offenlegung oder des unbefugten Zugriffs. Die Verordnung definiert allerdings nicht genau, wie eine Organisation diesen Schutz gewährleisten soll. Vielmehr müssen Unternehmen Kontrollen implementieren, die ihrem Risikograd «angemessen» sind – eine klare Anspielung auf risikobasierte Ansätze zur Cybersicherheit. Die DSGVO fordert somit eine grössere Konvergenz zwischen Cybersicherheit und Compliance, während diese beiden Bereiche von Unternehmen bislang häufig als unterschiedlich angesehen werden.

1.3 Internetseite

Ein wesentliches Element der Öffentlichkeitsarbeit ist der seit Oktober 2018 völlig neu konzipierte Internetauftritt sowie die mindestens zweimal monatlich versandten Newsletter der Datenschutzstelle. Die beiden Elemente sind insofern miteinander verbunden, als der Newsletter mit einem kurzen Überblick zum jeweiligen Thema auf neu bereitgestellte, weiterführende Informationen auf der Internetseite verweist. Erfreulicherweise stiegen die Zugriffszahlen im Berichtsjahr abermals deutlich an. Die meisten Zugrif-

fe auf die Internetseite wurden bei folgenden Beiträgen verzeichnet: Formulare und Downloads (15.7%), Für Unternehmen (7.3%), Veranstaltungen (7.3%), Berechtigtes Interesse (7.0%) sowie Videoüberwachung/Drohnen (6.7%).

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 etwa im Berichtsjahr ein Muster für ein Auskunftsersuchen gemäss Art. 15 DSGVO, das Meldeformular für die Videoüberwachung oder ein Musterbrief für Streitfälle in Bezug auf Videoüberwachungen im Nachbarschaftsbereich.

1.4 Newsletter

Bereits im Tätigkeitsbericht 2018 wies die Datenschutzstelle darauf hin, dass sie den E-Mail-Newsletter als wirksamen Kommunikationskanal erachtet und diesen im Berichtsjahr verstärkt zum Einsatz bringen würde. 2019 hat die Datenschutzstelle insgesamt 25 Newsletter versandt, was einer Steigerung um 50% entspricht. Im Schnitt über die letzten 12 Jahre waren es nur 14 versandte Newsletter pro Jahr. Ende 2019 hatten 1'014 Personen den Newsletter der Datenschutzstelle abonniert. Dies entspricht einem Plus von 199 Abonnenten gegenüber dem Vorjahr. Insbesondere bei den betrieblichen Datenschutzbeauftragten ist das Interesse am Newsletter der Datenschutzstelle gross. Aber auch im nahen Ausland stösst der Newsletter der Datenschutzstelle auf reges Interesse.

Die Themenbereiche der im Berichtsjahr von der Datenschutzstelle versandten 25 E-Mail-Newsletter umfassten beispielsweise Informationen zum neuen Angemessenheitsbeschluss der Europäischen Kommission für Japan, zur Videoüberwachung, zur Sicherheit von Passwörtern, zur Datenschutz-Folgenabschätzung, zum Auskunftsrecht, zu den berechtigten Interessen oder zum Datenschutz bei Direktwerbung. Bei der Wahl der Inhalte berücksichtigte die Datenschutzstelle soweit möglich die Bedürfnisse der Adressaten und reagierte auf verstärkte Anfragen zu bestimmten Themen. So arbeitete die Datenschutzstelle auf Anregung von betrieblichen Datenschutzbeauftragten etwa auch eine Checkliste für Benutzungsreglemente betreffend mobile Geräte oder eine Liste mit datenschutzrechtlichen «Dos and Don'ts im Büroalltag» aus. Gehäufte Anfragen zum Auskunftsrecht oder zum internationalen Datentransfer gaben ebenfalls Anlass zum Versand eines Newsletters und der Bereitstellung detaillierter Informationen dazu auf der Internetseite.

Sämtliche Newsletter können jederzeit auf der Internetseite der Datenschutzstelle nachgelesen werden, da der Inhalt der Newsletter dort Eingang in den Bereich «Themen A-Z» findet. Der Newsletter erlaubt somit seinen Abonnentinnen und Abonnenten, über Änderungen oder Neuerungen auf der Internetseite der Datenschutzstelle immer auf dem Laufenden zu sein, ohne die Internetseite in regelmässigen Abständen besuchen zu müssen.

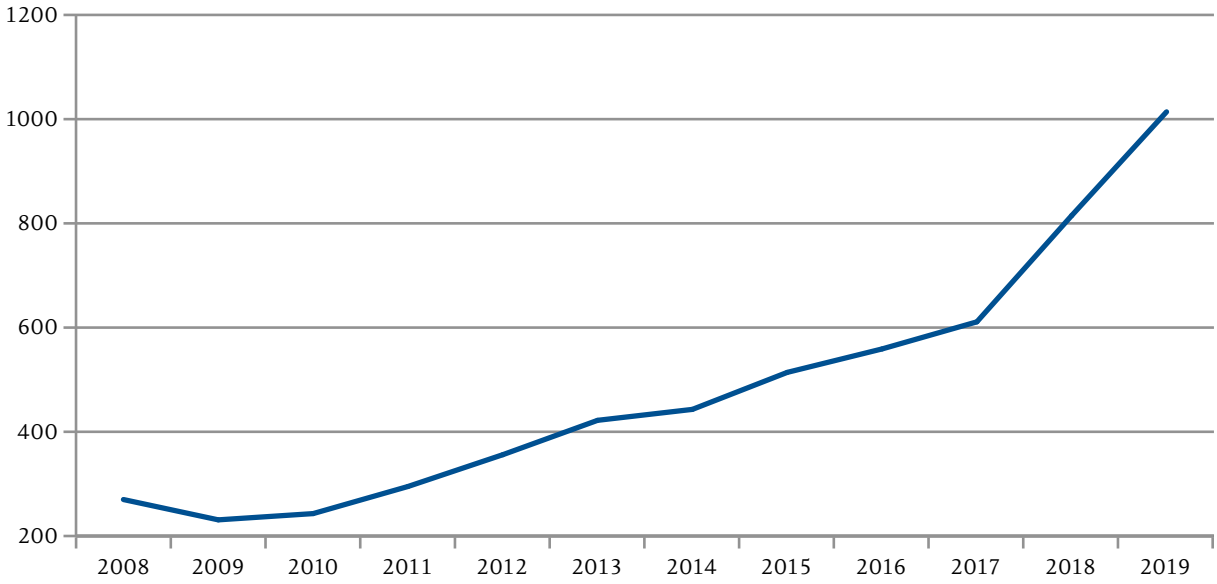


Abbildung 1: Entwicklung Newsletter Abonnenten

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

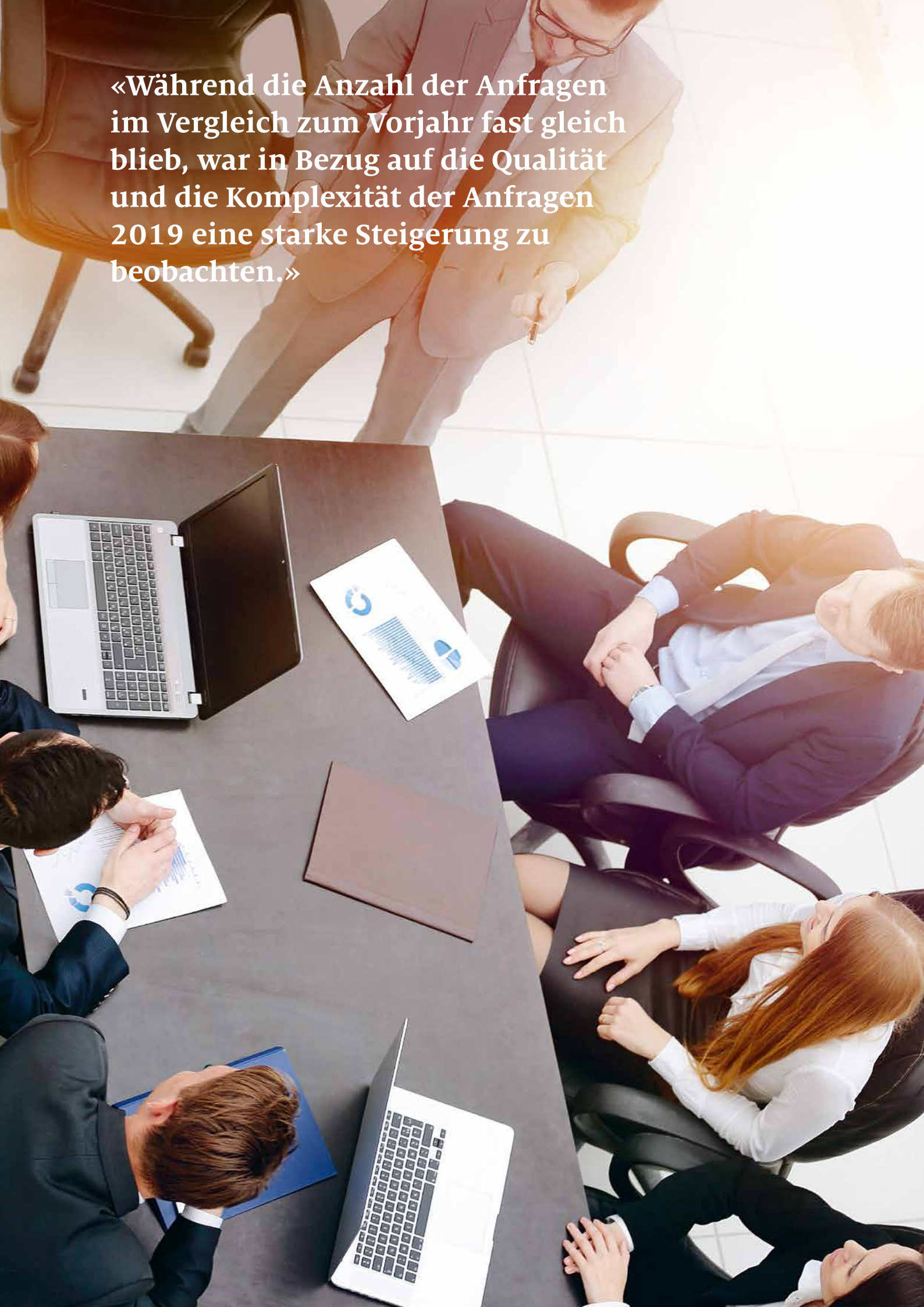
Die Beiträge werden vor allem auf unserer Internetseite gelesen. Der am meisten gelesene Newsletter im Berichtsjahr war «Selbstevaluation Datenschutz». Er wurde mehr als 500 Mal auf der Internetseite abgerufen. Zudem zählen zu den fünf am meisten gelesenen: «Neues Datenschutzgesetz in Kraft», «Neue Informationen zur Datenschutz-Folgenabschätzung (DSFA)», «Englische Versionen der wichtigsten Muster-Dokumente und Listen zum Datenschutz» sowie «Europäische Kommission erlässt Angemessenheitsbeschluss in Bezug auf Japan».

1.5 Datenschutz in den Medien

Im Berichtsjahr war der Datenschutz wieder prominent in den liechtensteinischen Medien vertreten, nur die Themen haben sich etwas geändert. Die knapp 20 Beiträge befassten sich unter anderem mit dem Datenschutztag 2019, Wildtierkameras, Drohnen, der Überwachung am Arbeitsplatz, der Digitalisierung der Stammbücher, der widerrechtlichen Weiterleitung von Nutzerdaten von Facebook, der Frage der Geldbussen unter der DSGVO in Europa und Liechtenstein, Erfahrungsberichten der Datenschutzstelle mit der Umsetzung der DSGVO, Cyber-Sicherheit oder automatisierten Fahrzeugen.

Auch im Ausland wurde die Datenschutzstelle von den Medien wahrgenommen. So erschien in der Juni Ausgabe der britischen Fachzeitschrift «Privacy Laws & Business» ein zweiseitiger Bericht über die Umsetzung der DSGVO im EWR-Staat Liechtenstein. Die Datenschutzstelle nutzte diese Gelegenheit um zu betonen, dass die DSGVO in den EWR-Staaten gleichrangig wie in der EU zur Anwendung kommt und die liechtensteinische Aufsichtsbehörde mit Ausnahme des vollen Stimmrechts im Europäischen Datenschutzausschuss über dieselben Befugnisse und Aufgaben verfügt wie die Aufsichtsbehörden in den EU-Mitgliedstaaten.

Aus Sicht der Datenschutzstelle ist die Berichterstattung in den Medien sowie deren positive Haltung gegenüber dem Datenschutz ein sehr wertvoller Beitrag zur Umsetzung des kommunikativen Konzepts der Datenschutzstelle, weil dadurch die Information gerade für Bürgerinnen und Bürger greifbar wird, die von Berufs wegen weniger Berührungspunkte mit dem Datenschutz haben.



«Während die Anzahl der Anfragen im Vergleich zum Vorjahr fast gleich blieb, war in Bezug auf die Qualität und die Komplexität der Anfragen 2019 eine starke Steigerung zu beobachten.»

2. Beratung in Bezug auf konkrete Anfragen

2.1 Allgemeines

Im Berichtsjahr 2019 verzeichnete die Datenschutzstelle 1'982 Anfragen von öffentlichen und privaten Institutionen. Im Vergleich zu den im Vorjahr beantworteten 2'004 Anfragen bedeutet dies lediglich einen marginalen Rückgang. Was die Qualität und die Komplexität der Anfragen betrifft, war 2019 hingegen eine starke Steigerung zu beobachten. Während im Vorjahr noch zahlreiche Fragen zur Geltung der DSGVO, dem Inkrafttreten des DSG oder der Bestellung eines Datenschutzbeauftragten innerhalb weniger Minuten beantwortet werden konnten, gab es im Berichtsjahr kaum eine Frage, die mit einem Zeitaufwand von unter einer Stunde zu erledigen war. Anstatt eine einfache, allgemein gültige Frage zu beantworten, ging es immer häufiger darum, einen komplexen Sachverhalt auf datenschutzrechtliche Fragestellungen zu überprüfen und in der Praxis umsetzbare Antworten und Lösungsansätze vorzulegen.

Mehraufwand entstand auch dadurch, dass die einzelnen Rückmeldungen koordiniert zu erfolgen hatten, um eine einheitliche Anwendung der DSGVO und des DSG durch die Datenschutzstelle zu gewährleisten. Hier erwies sich einmal mehr das Aktenverwaltungsprogramm LiVE als ein unverzichtbares Instrument. Mittels Schlagwortverzeichnis und einer sehr guten Suchfunktion war es jederzeit möglich, bei der Bearbeitung einer Anfrage auf bereits getroffene Entscheidungen zurückzugreifen und diese miteinander abzustimmen.

In Bezug auf die Herkunft der Fragestellenden war festzustellen, dass diese dem Trend des Vorjahres folgend zu einem grossen Teil aus der Privatwirtschaft stammten (49.5%). Die Mehrheit dieser Anfragen wiederum kam von kleinen und mittleren Unternehmen sowie Kleinstunternehmen. An zweiter bis vierter Stelle folgten die Landesverwaltung und die Gemeinden (20.8%), internationale Anfragen (11%) und die Vereine (7.8%). Auch Privatpersonen zeigten mit 7.6% der Anfragen erneut grosses Interesse an den Datenschutzbestimmungen. Lediglich die Medien waren im Berichtsjahr etwas zurückhaltender und stellten mit 66 Anfragen etwa ein Drittel weniger als im Vorjahr.

Beratungsanfragen konnten telefonisch, schriftlich – insbesondere mittels E-Mail – oder auch in einem persönlichen Gespräch bei der Datenschutzstelle eingebracht werden. Von den 1'982 Anfragen wurden im Berichtsjahr 413 telefonisch gestellt, währenddessen 2018 noch 687 Anrufer verzeichnet wurden. Die Begründung liegt auch hier wieder in der bereits erwähnten Zunahme der Komplexität der Fragestellungen, die einfache telefonische Anfragen und Auskünfte erschwerte.

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

2.2 Art. 15 DSGVO Auskunftsrecht

Eine der im Berichtsjahr am häufigsten gestellten Fragen betraf das Auskunftsrecht gemäss Art. 15 DSGVO. Während liechtensteinische Unternehmen 2018 nur von einzelnen praktischen Anwendungsfällen zum Art. 15 DSGVO berichteten, änderte sich die Situation 2019 deutlich und zahlreiche private wie vereinzelt öffentliche Stellen meldeten einen teils starken Anstieg der eingegangenen Auskunftsersuchen betroffener Personen. Insbesondere in Fällen, denen eine jahre- oder gar jahrzehntelange Kunden- bzw. Mitarbeiterbeziehung vorausgegangen war, zeigte sich die Schwierigkeit der Beantwortung solcher Ansuchen innerhalb der von der DSGVO vorgegebenen Frist.

Am meisten Kopfzerbrechen verursachte dabei das in Art. 15 Abs. 3 DSGVO festgehaltene Recht auf Kopie. Dieses kann von der betroffenen Person sowohl in Verbindung mit dem Recht auf Auskunft in Abs. 1 als auch isoliert geltend gemacht werden. Für Unsicherheit bei den Verantwortlichen sorgte hier jeweils der konkrete Umfang dieses Rechts bzw. die Frage, ob tatsächlich sämtliche Dokumente, E-Mails, Notizen etc., in denen etwa der Name und/oder sonstige personenbezogene Daten der betroffenen Person enthalten sind, herauszugeben sind. Eine weitere, regelmässig gestellte Frage betraf die Empfänger der Daten, welche ebenfalls gemäss Art. 15 DSGVO bekannt zu geben sind.

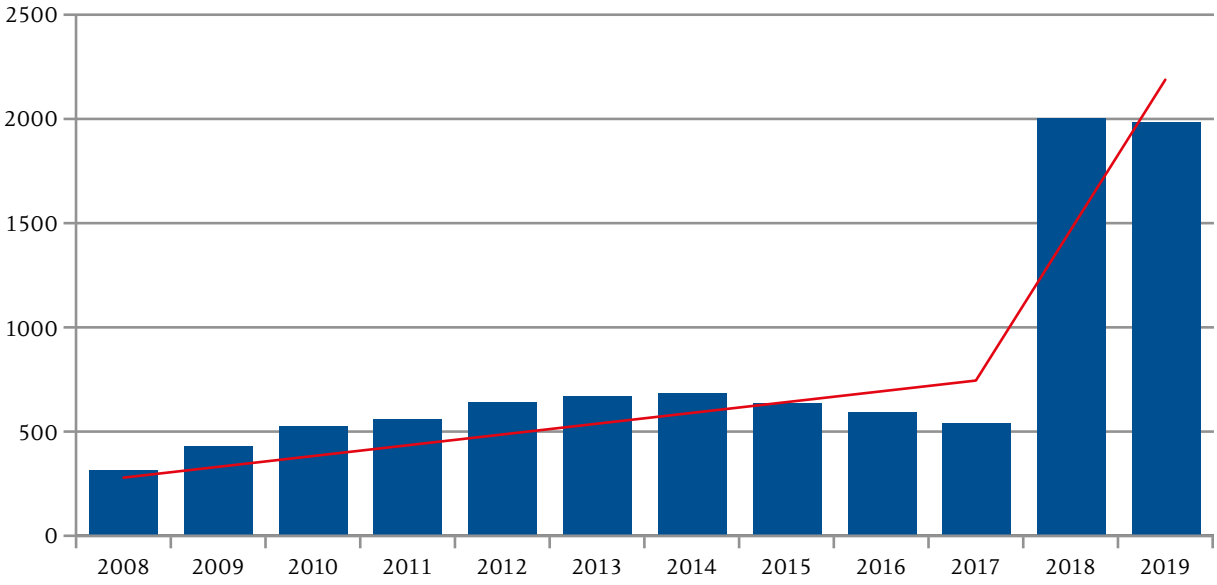


Abbildung 2: Anzahl der Anfragen von 2008 bis 2019

Für einige Unsicherheit in Liechtenstein sorgte zudem die Rechtsprechung in Deutschland zum Auskunftsrecht gemäss Art. 15 DSGVO. Da das deutsche Bundesdatenschutzgesetz als Rezeptionsgrundlage für das liechtensteinische DSG gewählt wurde und der Bericht und Antrag zum DSG an zahlreichen Stellen auf die «Lehre und Rechtsprechung aus dem Herkunftsland der Rezeptionsvorlage» verweist, stellte sich für viele Verantwortliche die Frage, ob und wie sie auf Urteile deutscher Gerichte zum Auskunftsrecht reagieren sollten. Erschwerend kam hinzu, dass diese Urteile nicht immer einheitlich sind, sondern diese einige Divergenzen untereinander aufweisen. Mehrere Unternehmen zeigten sich vor allem angesichts des Urteils des Landesarbeitsgerichts Baden-Württemberg vom 20. Dezember 2018 (Aktenzahl 17 Sa 11/18) besorgt. Die Richter hatten in diesem Fall entschieden, dass das beklagte Unternehmen dem Kläger nicht nur die Kategorien von Empfängern offenzulegen hat, sondern «die Empfänger» selbst. Daraus resultiert, dass eine betroffene Person Auskunft über jeden einzelnen Empfänger ihrer personenbezogenen Daten verlangen kann. Für Unternehmen kann sich eine entsprechende Auskunftserteilung in der Praxis jedoch als unrealisierbar erweisen. Zu denken sei etwa an ein Arbeitsverhältnis, im Laufe dessen die Daten über Jahre hinweg zum Beispiel zur Organisation von Dienstreisen an Dritte wie Fluggesellschaften, Hotels, Reisebüros etc. weitergegeben wurden.

In Bezug auf den Umfang des Rechts auf Kopie in Art. 15 Abs. 3 DSGVO ging das Urteil des Landesgerichts Köln vom 18. März 2019 (Aktenzahl 26 O 25/18) in eine andere Richtung und zeigte sich eher restriktiv. Nach Auffassung der Kammer bezieht sich der Auskunftsanspruch nicht auf sämtliche internen Vorgänge eines Verantwortlichen wie etwa interne Vermerke oder darauf, dass eine betroffene Person sämtlichen gewechselten Schriftverkehr, der ihr bereits bekannt ist, erneut ausgedruckt und übersendet erhalten kann. Rechtliche Bewertungen oder Analysen des Verantwortlichen stellen nach dieser Auffassung ebenfalls keine auskunftsberechtigten Daten dar.

Die Datenschutzstelle sprach sich im Berichtsjahr ebenfalls gegen eine extensive Auslegung des Auskunftsrechts aus, insbesondere im Hinblick auf die Frage der Empfänger gemäss Art. 15 Abs. 1 Bst. c DSGVO sowie bezüglich des Rechts auf Kopie gemäss Art. 15 Abs. 3 DSGVO. Abstrahiert von den konkreten Anlassfällen lassen sich die Feststellungen der Datenschutzstelle folgendermassen zusammenfassen:

- Die Auskünfte, die eine betroffene Person nach Art. 15 DSGVO verlangen kann, dienen primär dazu, ihr die Wahrnehmung der weiteren Rechte aus der DSGVO zu ermöglichen, also insbesondere das Recht auf Berichtigung nach Art. 16, auf Löschung nach Art. 17 und auf Einschränkung der Verarbeitung nach Art. 18.
- Soweit es sich um eine begrenzte Anzahl von Empfängern handelt, an die regelmässig Daten weitergegeben werden, sind diese namentlich zu erwähnen. Beispielsweise ein Lohn- oder Buchhaltungsbüro, Steuerberater oder Auftragsverarbeiter, mit denen langfristige Vertragsbeziehungen bestehen. Werden die Daten von Mitarbeitenden für die Organisation von

Geschäftsreisen an eine grosse Zahl von Reisedienstleistern wie Fluggesellschaften, Hotels, Verkehrsbetriebe etc. weitergegeben, genügt die Nennung der Kategorie von Empfängern.

– Das Recht auf Kopie umfasst nicht die Herausgabe einer *Fotokopie* sämtlicher Schriftstücke, in denen personenbezogene Daten der betroffenen Person erwähnt werden. Der Wortlaut *Kopie der personenbezogenen Daten* entspricht aus Sicht der Datenschutzstelle vielmehr einer geordneten Darstellung der personenbezogenen Daten, eine (Foto-)Kopie der Dokumente kann hingegen nicht der Regelfall sein. Dies steht auch im Einklang mit der Formulierung des Art. 12 Abs. 1 DSGVO, wonach der Verantwortliche durch geeignete Massnahmen alle Mitteilungen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln hat. Zudem ergibt sich aus der Gesetzessystematik, dass nur jene Kopien herauszugeben sind, die notwendig sind, damit die betroffene Person die Rechtmässigkeit der Verarbeitung ihrer Daten überprüfen und gegebenenfalls ihre Rechte wahrnehmen kann.
– Folglich müssen unternehmensinterne Gesprächsnotizen oder Sitzungsprotokolle, rechtliche oder andere spezifische Beurteilungen eines Sachverhalts in Bezug auf die betroffene Person, Telefonnotizen, Vertragsentwürfe (im Überarbeitungsmodus), sämtlicher E-Mailverkehr mit der betroffenen Person bzw. mit Dritten in Bezug und unter Erwähnung (einzelner) personenbezogener Daten der betroffenen Person nicht in Form einer (Foto-) Kopie herausgegeben werden.

2.3 Cookies

In seiner Pressemitteilung vom 1. Oktober 2019 zur Entscheidung in der Rechtssache *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e. V. gegen Planet49 GmbH* (C-673/17) stellte der EuGH fest:

«Mit seinem heutigen Urteil entscheidet der Gerichtshof, dass die für die Speicherung und den Abruf von Cookies auf dem Gerät des Besuchers einer Website erforderliche Einwilligung durch ein voreingestelltes Ankreuzkästchen, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss, nicht wirksam erteilt wird. [betrifft Frage 1. a) und c)]

Es macht insoweit keinen Unterschied, ob es sich bei den im Gerät des Nutzers gespeicherten oder abgerufenen Informationen um personenbezogene Daten handelt oder nicht. Das Unionsrecht soll den Nutzer nämlich vor jedem Eingriff in seine Privatsphäre schützen, insbesondere gegen die Gefahr, dass ‹Hidden Identifiers› oder ähnliche Instrumente in sein Gerät eindringen. [betrifft Frage 1. b)]

Der Gerichtshof stellt klar, dass die Einwilligung für den konkreten Fall erteilt werden muss. Die Betätigung der Schaltfläche für die Teilnahme am Gewinnspiel stellt deshalb noch keine wirksame Einwilligung des Nutzers in die Speicherung von Cookies dar.

Der Gerichtshof stellt ferner klar, dass der Diensteanbieter gegenüber dem Nutzer hinsichtlich der Cookies u.a. Angaben zur Funktionsdauer und zur Zugriffsmöglichkeit Dritter machen muss. [betrifft Frage 2.]»

Sowohl in der EU als auch in Liechtenstein als nicht EU-Staat löste das Urteil zahlreiche Diskussionen und nicht wenige Anfragen von privaten und öffentlichen Institutionen an die Datenschutzstelle aus. Die grundlegende Frage war, ob das Urteil in Liechtenstein überhaupt anwendbar ist. Die Antwort der Datenschutzstelle war klar, das Urteil kann in Liechtenstein keine Anwendung finden. Die Begründung liegt darin, dass die europäische Richtlinie, auf die sich das Urteil bezieht, nicht in den EWR übernommen wurde und somit in Liechtenstein keine Umsetzung im nationalen Recht erfahren hat. Der EWR bzw. Liechtenstein hat zwar die ursprüngliche Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation übernommen und im Kommunikationsgesetz umgesetzt, nicht aber die Revision dieser Richtlinie vom 25. November 2009 (Richtlinie 2009/136/EG). Jedoch erst die Revision 2009 verlangt für Cookies eine Einwilligung und bestimmt in ihrem Art. 5 Abs. 3, dass «*die Mitgliedstaaten sicherstellen, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäss der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine* Einwilligung *gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.*»

Mit der Revision 2009 wurde somit die noch in der Richtlinie 2002 verwendete Formulierung «*das Recht […], diese Verarbeitung zu* verweigern» durch den Begriff der «*Einwilligung*» ersetzt. Mangels Übernahme der revidierten Fassung von 2009 fand der Begriff der

Einwilligung jedoch keinen Eingang in das liechtensteinische Recht. Nachdem sich der EuGH in seinem Urteil *Planet49* ausschliesslich mit dem 2009 aufgenommen Begriff der Einwilligung auseinandersetzte, kann das Urteil in einer Rechtsordnung, die den Begriff nicht integriert hat, keine Anwendung finden.

Für die Betreiber einer Internetseite in Liechtenstein kann somit für die Frage, was bei der Verwendung von Cookies zu beachten ist, lediglich die DSGVO zum Tragen kommen. Und gemäss deren Art. 6 Abs. 1 Bst. f können neben der Einwilligung auch die berechtigten Interessen der Internetseiten-Betreiber eine Rechtsgrundlage bieten. In der Praxis heisst dies, dass von Internetseiten-Betreibern in Liechtenstein neben den unbedingt erforderlichen Cookies auch jene Cookies mit den berechtigten Interessen gerechtfertigt werden können, für die zwar keine unbedingte Erforderlichkeit besteht, bei denen jedoch die Interessen der Internetseiten-Betreiber höher zu gewichten sind als diejenigen der Internetseiten-Besucher.

Schliesslich ist auf eine weitere Besonderheit der liechtensteinischen Rechtsordnung hinzuweisen. Liechtenstein hat die Richtlinie 2002/58/EG als EU-Rechtsakt mit EWR-Relevanz zwar umgesetzt, allerdings aus Sicht der Datenschutzstelle keine korrekte Umsetzung des Art. 5 Abs. 3 vorgenommen. Art. 49 Kommunikationsgesetz regelt zwar unter dem Titel «Datenschutz» einzelne Aspekte der Datenverarbeitung, übernimmt aber im Gegensatz zu den meisten anderen EU- bzw. EWR-Staaten den Wortlaut des Art. 5 Abs. 3 der Richtlinie 2002/58/EG nicht in das nationale Gesetz.

Obgleich mittels Heranziehung der Bestimmungen der DSGVO eine datenschutzkonforme Lösung für die Beurteilung der Rechtsgrundlagen von Cookies in Liechtenstein erzielt werden kann, erachtet es die Datenschutzstelle für erforderlich, das Kommunikationsgesetz entsprechend zu revidieren, um die vollständige Umsetzung der Richtlinie 2002/58/EG zu gewährleisten.

2.4 Videoüberwachung

Mit Inkrafttreten des DSG am 1. Januar des Berichtsjahres erfuhr die Videoüberwachung öffentlich zugänglicher Räume in Art. 5 eine neue gesetzliche Regelung. So verwunderte es nicht, dass insbesondere die Anfragen zu diesem Themenbereich im Berichtsjahr sehr stark zunahmen. Eine Vielzahl der Anfragen konnte jedoch mit Verweis auf die ausführlichen Informationen auf der Internetseite der Datenschutzstelle und allgemeine Ausführungen zufriedenstellend beantwortet werden. Etwas komplizierter zu beantworten war die Frage nach der Definition des «öffentlich zugänglichen Raumes» für Eigentümer von Ein- oder Mehrfamilienhäusern. In diesen Fällen stellte die Datenschutzstelle klar, dass öffentlich zugänglicher Raum dort beginnt, wo es eine klare optische Abgrenzung zwischen dem zum Einfamilienhaus zugehörigen Grundstück und einer Strasse oder sonstigem öffentlichem Raum gibt.

Weitere Anfragen zur Videoüberwachung erreichten die Datenschutzstelle bezüglich der folgenden Themen:

- *Informationspflicht:* Die Datenschutzstelle stellt auf ihrer Internetseite ein Muster-Piktogramm zur Verfügung, welches in angepasster Form zur Information über eine Kamera vor Ort verwendet werden kann. Dabei ist für gewisse Teile der Information auch ein zweistufiges Verfahren erlaubt, in dem etwa per QR-Code auf eine entsprechende Internetseite mit den übrigen Datenschutzinformationen verwiesen wird.
- *Videokameras in Restaurants und Gaststätten sowie in Freizeiteinrichtungen:* Solche Kameras sind sehr heikel und regelmässig unzulässig, da es sich bei Gaststätten sowie Freizeiteinrichtungen um Orte handelt, an denen sich Personen zum sozialen und geselligen Austausch oder zur Ausübung von Freizeitaktivitäten aufhalten. Die Entfaltung der persönlichen Freiheit ist ein zentrales Grundrecht, welches gerade im Freizeitbereich durch die (gefühlte) Überwachung durch Kameras massgeblich beeinträchtigt wird.
- *Videoüberwachung am Arbeitsplatz:* Hier ist neben dem Datenschutz auch der Arbeitnehmerschutz betroffen. Überwachungen am Arbeitsplatz aller Art unterliegen sehr strengen Voraussetzungen und sind daher regelmässig als unzulässig anzusehen.
- *Webcams:* Diese sind grundsätzlich nur zulässig, wenn keine personenbezogenen Daten verarbeitet werden, sprich Personen oder die Kontrollschilder auf Autos nicht identifizierbar bzw. lesbar sind. Dies gilt auch für Kameras, die zur Verkehrs- oder Staubeobachtung an vielbefahrenen Strassen montiert werden. Für deren Zulässigkeit setzt die Datenschutzstelle daher voraus, dass ihr Aufnahmewinkel, Fokus oder ihre Schärfe so eingestellt sind, dass weder die Kontrollschilder noch die Lenkerinnen oder Lenker erfasst werden.
- *Dash-Cams:* In ihrer Stellungnahme zum Bericht und Antrag des neuen DSG hat die Datenschutzstelle unter Berufung auf ihre bis dahin getätigten Stellungnahmen Dash-Cams noch als unzulässig

eingestuft. Mittlerweile hat die Datenschutzstelle diese Meinung aufgrund eines Urteils des deutschen Bundesgerichtshofes und der angepassten Praxis der österreichischen Datenschutzaufsichtsbehörde revidiert. Dash-Cams, die umfassende und eingrenzende Voraussetzungen erfüllen, können als zulässig erachtet werden. In der Praxis bedeutet dies, dass es zu keiner dauerhaften Aufzeichnung kommen darf, sondern lediglich die kurzzeitige anlassbezogene Speicherung im Zusammenhang mit einem Unfallgeschehen als zulässig eingestuft wird. Weiter sind Massnahmen gemäss Art. 25 DSGVO zu ergreifen, wie etwa eine Verpixelung der Personen oder ein automatisiertes und dem Eingriff des Verwenders entzogenes Löschen der Aufnahmen. Selbst in diesem sehr engen Anwendungsbereich ist die Zulässigkeit von Dash-Cams nach wie vor kritisch zu sehen, nicht zuletzt deshalb, weil die Informationspflicht nach Art. 13 DSGVO in der Praxis eine Herausforderung darstellt.

– *Wildtierkameras:* Die Problematik bei solchen Kameras ist jeweils, dass bei nicht korrekter Kennzeichnung und Information der verantwortliche Betreiber kaum ausfindig gemacht werden kann. Dabei sind gerade Wildtierkameras, welche in Wander- und Naturgebieten angebracht werden, datenschutzrechtlich brisant. Denn diese erfassen einen Bereich, welcher von der Bevölkerung zur Freizeitgestaltung genutzt wird und somit grundsätzlich auch nicht ohne einen konkreten Grund überwacht werden darf. Um die Privatsphäre der Personen zu respektieren, die sich zu Freizeit- und Erholungszwecken im Wald aufhalten, sind Wildtierkameras so einzustellen, dass die Rechte betroffener Personen nicht verletzt werden. Ebenso wesentlich ist eine korrekte Information gemäss Art. 13 DSGVO, die vor allem auch den Verantwortlichen und seine Kontaktdaten präzise und transparent kommuniziert. Im Berichtsjahr erörterte die Datenschutzstelle diese Pflichten vor allem mit der zuständigen Stelle im Amt für Umwelt und wies auf die Notwendigkeit einer datenschutzkonformen Ausgestaltung der von ihnen betriebenen Wildtierkameras hin.
– *Drohnen mit Videokameras:* Diesbezügliche Anfragen (und Beschwerden) waren im Berichtsjahr leicht rückläufig und betrafen praktisch ausschliesslich Drohnenflüge für gewerbliche Zwecke wie die Kontrolle des Baustellenfortschritts, Kontrollen von Gebäudedächern, Grundstückserfassungen oder Werbezwecke. Aufnahmen von Videokameras mittels Drohnenflügen sind grundsätzlich meldepflichtig, wenn eine Verarbeitung personenbezogener Daten nicht ausgeschlossen werden kann. Da Drohnen aber auch noch andere wichtige Rechtsbereiche tangieren, fand im Berichtsjahr erneut ein Treffen zwischen Vertretern der Landespolizei, des Amtes für Bau und Infrastruktur sowie der Datenschutzstelle statt.

Bei zahlreichen Anfragen und Beschwerden zur Zulässigkeit von Videoüberwachungen nahm die Datenschutzstelle auch Besichtigungen und Besprechungen vor Ort wahr. Dabei wurde bei einigen Videoüberwachungssystemen die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) festgestellt. An dieser Stelle möchte die Datenschutzstelle hervorheben, dass insbesondere für systematische, umfangreiche (weiträumige) Videoüberwachungen öffentlich zugänglicher Bereiche eine DSFA gemäss Art. 35 Abs. 3 Bst. c DSGVO zwingend erforderlich ist und von den Betreibern jeweils vor Inbetriebnahme des Videoüberwachungssystems durchzuführen ist.

In Bezug auf die neu mit Art. 5 Abs. 7 DSG sowie Art. 5 DSV eingeführte Meldepflicht von Videoüberwachungsanlagen sind im Berichtsjahr elf Drohnenflüge, ein Projekt mit mehreren Wildtierkameras sowie 23 stationäre Videoüberwachungen bei der Datenschutzstelle gemeldet worden.

2.5 Einwilligungserfordernis bei Familien- und Firmenchronik

Eine Privatperson fragte bei der Datenschutzstelle an, ob für die Erstellung einer Familien- und Firmenchronik, in der Fotos von privaten Personen aus dem Freundeskreis und aus geschäftlichen Beziehungen in einem Buch abgedruckt werden sollen, entsprechende Einwilligungen der abgebildeten Personen einzuholen sind. Es sei geplant, dieses Buch nur Familienfreunden und einigen Geschäftspartnern anlässlich einer Feierlichkeit zu schenken. Die Privatperson wurde von der Datenschutzstelle darüber informiert, dass das Vorhaben nur rechtmässig ist, wenn die Betroffenen vorgängig in die Verarbeitung ihrer personenbezogenen Daten für die Erstellung der Familien- und Firmenchronik (idealerweise schriftlich) einwilligen. Wesentlich ist, dass die Betroffenen wissen, worin sie einwilligen – man spricht von einer «informierten Einwilligung». Art. 2 Abs. 2 Bst. c DSGVO kennt zwar für die Datenverarbeitung durch Privatpersonen ausschliesslich für persönliche oder familiäre Tätigkeiten – ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit – die sogenannte Haushaltsausnahme als Ausnahmevorschrift (Anwendbarkeit der DSGVO wäre ausgeschlossen). Diese Ausnahmeregelung ist

jedoch sehr eng auszulegen. Es werden demnach nur solche Verarbeitungen des Privat- oder Familienlebens von Einzelpersonen erfasst, die objektiv betrachtet «ausschliesslich» persönlicher oder familiärer Art sind. Schlüsselkriterium ist somit die Zurechenbarkeit zum privaten Bereich. Dabei ist in der Folge der Adressatenkreis zu beurteilen. Bei allgemein zugänglicher Veröffentlichung ohne jegliche Beschränkung kann diese Ausnahme somit nicht in Anspruch genommen werden. Als Beispiel wird in den Kommentaren der Vergleich zwischen einer privaten Facebook-Seite mit überschaubarer Anzahl von Freunden, Fotos und Videos (Haushaltsausnahme greift) und dem gleichen Inhalt auf einem öffentlichen zugänglichen Account (Haushaltsausnahme greift nicht) gezogen.

2.6 Verbindliche interne Datenschutzvorschriften

Im Berichtsjahr bekundete ein weltweit tätiges, liechtensteinisches Unternehmen Interesse an der Ausarbeitung von verbindlichen internen Datenschutzvorschriften für sämtliche seiner Unternehmenseinheiten *(binding corporate rules; BCR)*. Die Datenschutzstelle fungiert im Rahmen dieses laufenden EWR-weiten Bewilligungsverfahrens als federführende Behörde. Das besagte Unternehmen hat im Berichtsjahr mit der konkreten Ausarbeitung seiner BCR begonnen und wird dabei von der Datenschutzstelle wo nötig beraten.

2.7 Technischer Datenschutz

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

Ist die Verschlüsselung des Datenverkehrs von Internetauftritten, beispielsweise mittels HTTPS, in allen Fällen verpflichtend?

Gemäss Art. 5 Abs. 1 Bst. f DSGVO muss durch geeignete technische und organisatorische Massnahmen eine angemessene Sicherheit, insbesondere Integrität und Vertraulichkeit, der Verarbeitung personenbezogener Daten gewährleistet sein. Datensicherheit ist somit ein Grundsatz jeder Verarbeitung personenbezogener Daten. HTTPS, meist gekennzeichnet durch ein Schlosssymbol im Bereich der Adressleiste des Browsers, gewährleistet durch die Verwendung kryptographischer Protokolle Integrität und Vertraulichkeit in der Kommunikation zwischen Webserver und dem Webbrowser (Transportverschlüsselung) und stellt somit eine geeignete technische Massnahme im Sinne der Datensicherheit gemäss Art. 32 DSGVO dar. Ohne HTTPS werden sämtliche Daten, die auf einer Internetseite abgerufen oder übermittelt werden, wie beispielsweise Benutzernamen und Passwörter, Kreditkartendaten oder Eingaben in Formulare, unverschlüsselt übertragen. Während dieser unverschlüsselten Übertragung besteht die Gefahr einer unbefugten Einsichtnahme oder anderweitigen unrechtmässigen Verarbeitung. Somit ist in jenen Fällen, in denen auf der Internetseite personenbezogene Daten ausgetauscht werden, wie bei der Verwendung von Logins, Kontaktformularen, in Onlineshops etc., eine dem Stand der Technik entsprechende und verschlüsselte Übertragung der Internetseiteninhalte sicherzustellen. Wenn jedoch keine personenbezogenen Daten verarbeitet oder übertragen werden, könnte der Verantwortliche grundsätzlich auf eine Transportverschlüsselung verzichten. Da zwischenzeitlich– bis auf wenige Ausnahmen – sämtliche Hoster und Anbieter von Webseitenbaukästen den Kunden HTTPS anbieten, sollten und werden moderne unverschlüsselte Webauftritte eher die Ausnahme sein.

Kann ein Office-Dokument ohne die Beschaffung zusätzlicher und kostenintensiver Sicherheitssoftware datenschutzkonform per E-Mail an einen oder mehrere Empfänger übermittelt werden?

Der Verantwortliche kann aufgrund des festgestellten Schutzniveaus bei der Übermittlung von personenbezogenen Daten via E-Mail dazu verpflichtet sein, eine Ende-zu-Ende Verschlüsselung als technische Massnahme im Sinne des Art. 32 DSGVO für die Inhalte von E-Mails zu verwenden. Doch dies ist aus bestimmten Gründen nicht immer möglich, etwa weil den Empfängern die dafür notwendige Infrastruktur nicht zur Verfügung steht. In diesen Fällen kann alternativ eine E-Mail mit verschlüsseltem Anhang versendet werden. Dabei ist zu beachten, dass im E-Mail-Text selbst keine vertraulichen Inhalte vorhanden und Anhänge entsprechend stark verschlüsselt sind. AES-verschlüsselte Zip-Archive oder Dokumente, wie sie von gängiger Büro- und Archivsoftware erstellt werden können, sind Beispiele hierfür. Wichtig ist dabei darauf zu achten, dass das zur Entschlüsselung notwendige Passwort nur dem Absender und den befugten Empfängern bekannt ist und sämtlichen Kriterien für starke und sichere Passwörter entspricht (ausreichende Passwortlänge, enthält Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen etc.). Schliesslich ist sicherzustellen, dass den Empfängern das Passwort nicht ebenso über E-Mail, sondern über einen anderen Kanal, etwa telefonisch oder mit einer Textnachricht (SMS), übergeben wird. Die Datenschutzstelle rät jedoch lediglich für einmalige oder seltene Übermittlungen mit wechselnden Empfängern, die nicht über eine Verschlüsse-

lungsinfrastruktur verfügen, zu dieser Art der Vorgehensweise, wie zum Beispiel für die Übermittlung von Daten an betroffene Personen nach einem Auskunftsgesuch gemäss Art. 15 DSGVO. Für die regelmässige Kommunikation sollten andere Lösungen in Betracht gezogen werden.

Ist beim Einsatz biometrischer Zutrittssysteme zu speziell gesicherten Bereichen in Unternehmen in allen Fällen gemäss Art. 35 DSGVO eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen?
Zweck der DSFA ist es, im Falle von besonders riskanten Datenverarbeitungsvorgängen die voraussichtlichen Risiken für die persönlichen Rechte und Freiheiten betroffener Personen zu identifizieren und zu bewerten, um diese schliesslich mit entsprechenden Massnahmen reduzieren zu können. Eine Verpflichtung zur Durchführung einer DSFA besteht im Falle einer riskanten Datenverarbeitung gemäss Art. 35 Abs. 1 DSGVO sowie im Falle der in Abs. 3 genannten Beispiele, die jedoch nicht als abschliessende Aufzählung zu betrachten sind. Die erwähnten Absätze enthalten allgemeine Regelungen und werden durch die Liste der Verarbeitungstätigkeiten der Datenschutzstelle gemäss Art. 35 Abs. 4 DSGVO ergänzt, die auf der Internetseite der Datenschutzstelle eingesehen und heruntergeladen werden kann. Für sämtliche auf dieser Liste beschriebene Verarbeitungsvorgänge ist die Durchführung einer DSFA obligatorisch. So verpflichtet etwa Punkt 8 der Liste, dass bei der Verarbeitung von biometrischen Daten im Sinne von Art. 4 Ziff. 14 DSGVO zur eindeutigen Identifizierung natürlicher Personen eine DSFA durchzuführen ist, *wenn* zusätzlich mindestens ein weiteres Kriterium der europäischen Leitlinien zur Datenschutz-Folgenabschätzung[1] erfüllt ist. Das einzige im gegenständlichen Sachverhalt passende weitere Kriterium ist der Umfang der Datenverarbeitung. Die Leitlinien empfehlen die Berücksichtigung speziell folgender Faktoren, wenn ermittelt werden soll, ob eine fragliche Verarbeitung in grossem Umfang durchgeführt wird: a) die Zahl der betroffenen Personen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe; b) die verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente; c) die Dauer oder Dauerhaftigkeit der Datenverarbeitung sowie d) das geografische Ausmass der Datenverarbeitung. Gemäss Art. 32 iVm Art. 5 Abs. 1 Bst. f DSGVO ist bei der Vergabe von Zutrittsrechten in gesicherte Bereiche Zurückhaltung geboten. Bei den Anfragen an die Datenschutzstelle waren die Anzahl der betroffenen Personen sowie der Umfang der verarbeiteten Daten jeweils gering. Somit lag keine umfangreiche Verarbeitung vor. Im Ergebnis hielt die Datenschutzstelle gegenüber dem Verantwortlichen fest, dass die alleinige Verwendung von biometrischen Merkmalen zwecks Zutrittssicherung ohne weitere Datenverarbeitung und im eingeschränkten Umfang vom Punkt 8 der Liste nach Art. 35 Abs. 4 DSGVO nicht erfasst wird. Es bestand somit keine Verpflichtung zur Durchführung einer DSFA. Dagegen wird in Fällen, in denen ein Unternehmen flächendeckend Fingerabdrucksensoren oder andere Scanner einsetzt, der grosse Umfang der Datenverarbeitung regelmässig zu bejahen und somit die Durchführung einer DSFA notwendig sein.

Gibt es in der DSGVO oder dem DSG eine Bestimmung, die vorschreibt oder festlegt, wie lange personalisierte Aufzeichnungen von Zutrittsdaten in einem Gebäude gespeichert werden müssen bzw. dürfen? Erfasst wurde im konkreten Fall, wer wann und um welche Zeit welche Türe öffnete. Falls nein, wie lange dürfen solche Protokolle gespeichert werden?
Im Zusammenhang mit Aufbewahrungsfristen von Protokolldaten kommt es vor allem auf den Zweck der konkreten Datenverarbeitung an. Weswegen werden die Zutrittsdaten/Protokolle gespeichert? Ein möglicher legitimer Zweck ist die Sicherstellung und Prüfbarkeit der Integrität und Vertraulichkeit der Datenverarbeitung innerhalb eines Unternehmens (Zutrittskontrolle). Der Zutritt zu Bereichen, in denen personenbezogene Daten verarbeitet oder gespeichert werden, sollte mittels geeigneter Zutrittssteuerungen, wie zum Beispiel einer Zutrittskarte oder einer geheimen PIN, befugten Personen vorbehalten werden. Ebenso sollten ein physisches Protokollbuch oder eine elektronische Dokumentation existieren, die sicher aufbewahrt und bei Bedarf ausgewertet werden können. Das Protokoll adressiert somit die Anforderung der DSGVO in Bezug auf die Nachweisbarkeit der Datensicherheit. Doch was die Aufbewahrungsfrist solcher Protokolle betrifft, macht die DSGVO keine konkreten Angaben. Hier kann der Verantwortliche sich an anderen bestehenden Fristen im Zusammenhang mit (Datensicherheits-)Protokollen orientieren. So sieht zum Beispiel Art. 75 Abs. 4 DSG bei der Aufbewahrung von Protokollen – im Zusammenhang mit der Verarbeitungen zu Zwecken nach Art. 1 Abs. 1 der Richtlinie (EU) 2016/680 – vor, dass die Protokolldaten am Ende des auf deren Generierung folgenden Jahres zu löschen sind. Somit scheint eine Aufbewahrung der Protokolle von einem Jahr durchaus verhältnismässig und mit der

1 Leitlinien zur Datenschutz-Folgenabschätzung der ehemaligen Artikel-29-Datenschutzgruppe, WP 248 Rev. 01 in der Version vom 4. Oktober 2017.

DSGVO vereinbar. Was den Zugriff auf die Protokolle betrifft, ist im Sinne des Art. 32 DSGVO ausschliesslich jene Personengruppe zugriffsberechtigt, die für die Zutrittssicherheit oder auch die Überprüfung der Rechtmässigkeit der Datenverarbeitung verantwortlich zeichnet (Zweckbindung in Bezug auf das Protokoll). Der Zugriff auf die gespeicherten Protokolldaten sollte entsprechend geregelt und auch dokumentiert werden.

2.8 Anwendungsfragen zum DSG und zur DSV

Anfragen zur Anwendung des DSG und der DSV kamen vor allem von öffentlichen Stellen und bezogen sich zu einem grossen Teil auf die Art. 22 und 24 DSG betreffend die Verarbeitung zu anderen Zwecken durch öffentliche Stellen bzw. Datenübermittlungen durch öffentliche Stellen. Beide Bereiche waren in der Vergangenheit von den einzelnen Amtsstellen unterschiedlich und nach eigenem Ermessen gehandhabt worden. Mit Art. 22 und 24 DSG haben diese besonderen Verarbeitungsvorgänge nun nach einheitlichen Massstäben und unter recht engen Voraussetzungen zu erfolgen. Einzelne Ämter entwickelten ein grosses Problembewusstsein und passten ihre Praxis unverzüglich an die neuen Bestimmungen an. Beispielgebend kann etwa das Amt für Umwelt genannt werden, das regelmässig mit zahlreichen Anfragen zur Datenbekanntgabe konfrontiert ist. Die fraglichen Praxisfälle wurden bis zum Amtsantritt der behördlichen Datenschutzbeauftragten im September 2019 mit der Datenschutzstelle diskutiert und das Amt bei der Ausarbeitung einer einheitlichen Praxis unterstützt.

Beispielsweise wollte eine Privatperson vom Amt für Umwelt Auskunft darüber erhalten, von wem drei bestimmte Grundstücksparzellen bewirtschaftet werden und welche staatlichen Beiträge der jeweilige Bewirtschafter dafür erhält. Die anfragende Person ist selbst Eigentümer von zwei der drei Parzellen, in Bezug auf die dritte Parzelle sind ihr die Eigentumsverhältnisse dagegen nicht bekannt. Theoretisch sind die Beiträge aus zwei Verordnungen herauslesbar, aus der Landwirtschafts-Bewirtschaftungs-Förderungs-Verordnung (LBFV) und der Landschaftspflege-Förderungs-Verordnung (LPFV). Mangels bestimmter Zusatzinformationen ist eine genaue Berechnung für die anfragende Person jedoch kaum möglich.

Gemäss Art. 24 DSG ist die Übermittlung personenbezogener Daten durch öffentliche Stellen an nicht-öffentliche Stellen zulässig, wenn:

«a) sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach Art. 22 zulassen würden;

b) der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat; oder

c) sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.»

Im vorliegenden Fall könnte angenommen werden, dass für die ersten beiden Grundstücksparzellen Bst. b zutrifft und die gewünschte Information daher vom Amt der anfragenden Person übermittelt werden darf. In Bezug auf das fremde Grundstück war im konkreten Fall abzuwägen, ob es Alternativen zur Offenlegung durch das Amt für Umwelt gab. Dies wäre etwa der direkte Kontakt des Anfragenden mit dem Eigentümer. Die Datenschutzstelle sah diese Alternative als Grund, die Herausgabe der Information durch das Amt für Umwelt nicht zu empfehlen.

In Bezug auf die Rechte der Betroffenen gemäss Art. 32 bis 37 DSG gab es lediglich vereinzelte Anfragen an die Datenschutzstelle. Hier zeigte sich, dass die Betroffenenrechte der DSGVO in der Praxis im Vordergrund standen und sich die Anfragen fast ausschliesslich auf die DSGVO bezogen.

«Die Datenschutzstelle ist überzeugt, dass die Kontrolle über die eigenen Daten im Sinne einer tatsächlichen Datensouveränität zu Vertrauen der betroffenen Personen gegenüber dem E-Government führen wird.»

3. Stellungnahmen zu Vorlagen und Erlassen

3.1 Stellungnahme RVOG

Mit der Revision des Gesetzes über die Regierungs- und Verwaltungsorganisation (RVOG) wurde unter anderem die Umsetzung des sogenannten Once-Only-Prinzips angestrebt, welches in der Tallinn Declaration on eGovernment vom Oktober 2017 postuliert wird. Mit der Tallinn Declaration on eGovernment wurde auf Initiative der damaligen estnischen EU-Ratspräsidentschaft von 32 jeweils für die Digitalpolitik zuständigen Ministern aus den EU- und EFTA-Staaten eine Erklärung mit Zielsetzungen unterzeichnet, die auf dem «EU eGovernment Action Plan 2016–2020» beruhen.

Ziel des Once-Only-Prinzips ist, dass Bürgerinnen und Bürger sowie Unternehmen bestimmte Standardinformationen der Verwaltung nur einmal zur Verfügung stellen müssen und die einzelnen Verwaltungseinheiten dann die Informationen untereinander austauschen. Dadurch sollen administrative Belastungen der Bürgerinnen und Bürgern sowie der Unternehmen bei der Kommunikation mit der öffentlichen Verwaltung verringert werden. Nach Ansicht der Datenschutzstelle kann dieses Vorhaben nur gelingen, wenn entsprechende Rahmenbedingungen geschaffen werden, die es den Bürgerinnen und Bürgern erlauben, die Hoheit über ihre personenbezogenen Daten zu behalten, indem ihnen Kontrollmöglichkeiten zur Verfügung stehen und sie die Übersicht behalten, was mit ihren Daten geschieht und wer auf sie Zugriff hat. Nur mit einem verantwortungsvollen Umgang der Verwaltung mit den personenbezogenen Daten der Bürgerinnen und Bürger in Übereinstimmung mit den Datenschutzbestimmungen kann ein solches Projekt erfolgreich implementiert werden.

Die Umsetzung des Once-Only-Prinzips – und damit eines umfassenden E-Governments – baut auf der Idee auf, dass die personenbezogenen Daten der Bürgerinnen und Bürger an einem zentralen Ort gespeichert werden, wo sie von diesen auch verwaltet werden können. Die DSGVO macht für die weitere Verarbeitung personenbezogener Daten aus solch einer zentralen, staatlichen Datenbank eine Reihe von Vorgaben und verlangt insbesondere das Vorliegen einer Rechtsgrundlage im Sinne des Art. 5 Abs. 1 Bst. a in Verbindung mit Art. 6 Abs. 1 bzw. Art. 9 Abs. 2 DSGVO. Im Einzelfall kann dies eine spezielle gesetzliche Ermächtigung sein, etwa im Sinne der Art. 22 oder 24 DSG oder eines anderen Spezialgesetzes. Soweit eine solche aber fehlt, ist die Verarbeitung der personenbezogenen Daten durch eine andere öffentliche Stelle nur zulässig, wenn die Bürgerin oder der Bürger ihre bzw. seine Einwilligung dafür gegeben hat. Idealerweise sollte daher den betroffenen Personen bereits beim ersten Kontakt mit der Verwaltung die Möglichkeit gegeben werden, etwa im Rahmen eines Bürgerportals, eine klare, unmissverständliche Einwilligung in verschiedene staatliche Datenverarbeitungen abzugeben. Diese Einwilligung erlaubt es in der Folge den verschiedenen Verwaltungseinheiten, auf die zentral gespeicherten Daten zuzugreifen und für ihre eigenen Zwecke (weiter) zu verarbeiten. Ein solches Bürgerportal muss zudem umfassende und transparente sowie leicht zugängliche und verständliche Informationen über die Datenverarbeitung im Sinne des Art. 13 DSGVO beinhalten. Denn damit wird sichergestellt, dass sich die betroffene Person der Tragweite ihrer Entscheidung bereits bei Einwilligungserteilung bewusst ist.

In ihrem Vernehmlassungsbericht führt die Regierung unter Punkt «3.2 Datenverarbeitung» aus, dass es das Ziel der Vorlage ist, eine Konkretisierung von Art. 4 DSG vorzunehmen. Darunter versteht die Vorlage sowohl die Verarbeitung der von öffentlichen Stellen für einen eigenen Zweck erhobenen Daten als auch die künftige Weiterverwendung der Daten durch andere öffentliche Stellen zu deren eigenen Zwecken.

Die Datenschutzstelle ist hier jedoch der Auffassung, dass sich Art. 4 DSG nicht auf eine Weiterverwendung von personenbezogenen Daten bezieht, die ursprünglich zu einem anderen Zweck und somit der Erfüllung einer anderen öffentlichen Aufgabe erhoben wurden. Dieser Sachverhalt findet eine Regelung in Art. 22 DSG oder Art. 6 Abs. 4 DSGVO. Art. 22 Abs. 1 DSG listet in den Bst. a bis f explizit auf, in welchen Fällen eine solche Weiterverwendung zulässig ist. Zu bedenken ist allerdings, dass Art. 22 DSG im Regelfall davon ausgeht, dass die Weiterverwendung durch dieselbe Behörde, allerdings zu einem anderen Zweck, vorgenommen wird. Folglich ist es unumgänglich, auch Art. 24 DSG zu prüfen, welcher Datenübermittlungen durch öffentliche Stellen an andere öffentliche Stellen regelt. Da allerdings Art. 24 Abs. 1 DSG wiederum für die Zulässigkeit der Übermittlung auf Art. 22 DSG verweist, müssen auch hier die Voraussetzungen des Art. 22 Abs. 1 Bst. a bis f DSG geprüft werden.

Die Stellungnahme der Datenschutzstelle und ihre eindringliche Aufforderung, das RVOG entsprechend der Datenschutzgesetzgebung zu revidieren, findet auch Rückhalt im *EU-eGovernment-Aktionsplan*

2016–2020 zur Beschleunigung der Digitalisierung der öffentlichen Verwaltung, welcher ebenfalls die Bedeutung des Datenschutzes und der Privatsphäre beim Ausbau von E-Government-Architekturen betont, indem er diese beiden Aspekte explizit miteinander in Verbindung bringt:

«Grundsatz der einmaligen Erfassung: Öffentliche Verwaltungen sollten sicherstellen, dass die Menschen und Unternehmen ihnen dieselben Informationen nur einmal übermitteln. Soweit zulässig, sollten sie diese Daten – unter vollständiger Beachtung der Datenschutzvorschriften – intern mehrmals verwenden, um eine unnötige zusätzliche Belastung der Bürgerinnen und Bürger und der Unternehmen zu vermeiden.»

Eine funktionierende digitale Verwaltung, die auf Grundsätze wie das Once-Only-Prinzip setzt, verarbeitet eine beträchtliche Menge personenbezogener Daten der teilnehmenden Bürgerinnen und Bürger an zentraler Stelle mit Zugriffsrechten unterschiedlichster Behörden. Die Datenschutzstelle ist überzeugt, dass nur das Gefühl der Kontrolle über die eigenen Daten im Sinne einer tatsächlichen Datensouveränität zu Vertrauen und Offenheit der betroffenen Personen gegenüber dem E-Government führen wird und einzig dadurch das Projekt zu einem Erfolg werden kann.

Wenn insbesondere Basisdaten wie Name, Geburtsort und -datum, Meldeadresse etc. für alle Ämter sowie weitere, eng an die Landesverwaltung angeschlossene Verwaltungseinheiten jederzeit verfügbar sein können, erscheint es aus Sicht der Datenschutzstelle wesentlich, dass anschliessend an die Revision des RVOG noch eine zusätzliche datenschutzkonforme Rechtsgrundlage in Form einer (Total-)Revision des Gesetzes über das Zentrale Personenregister (ZPRG) für die neue Applikation geschaffen wird.

3.2 Stellungnahme E-Government-Gesetz

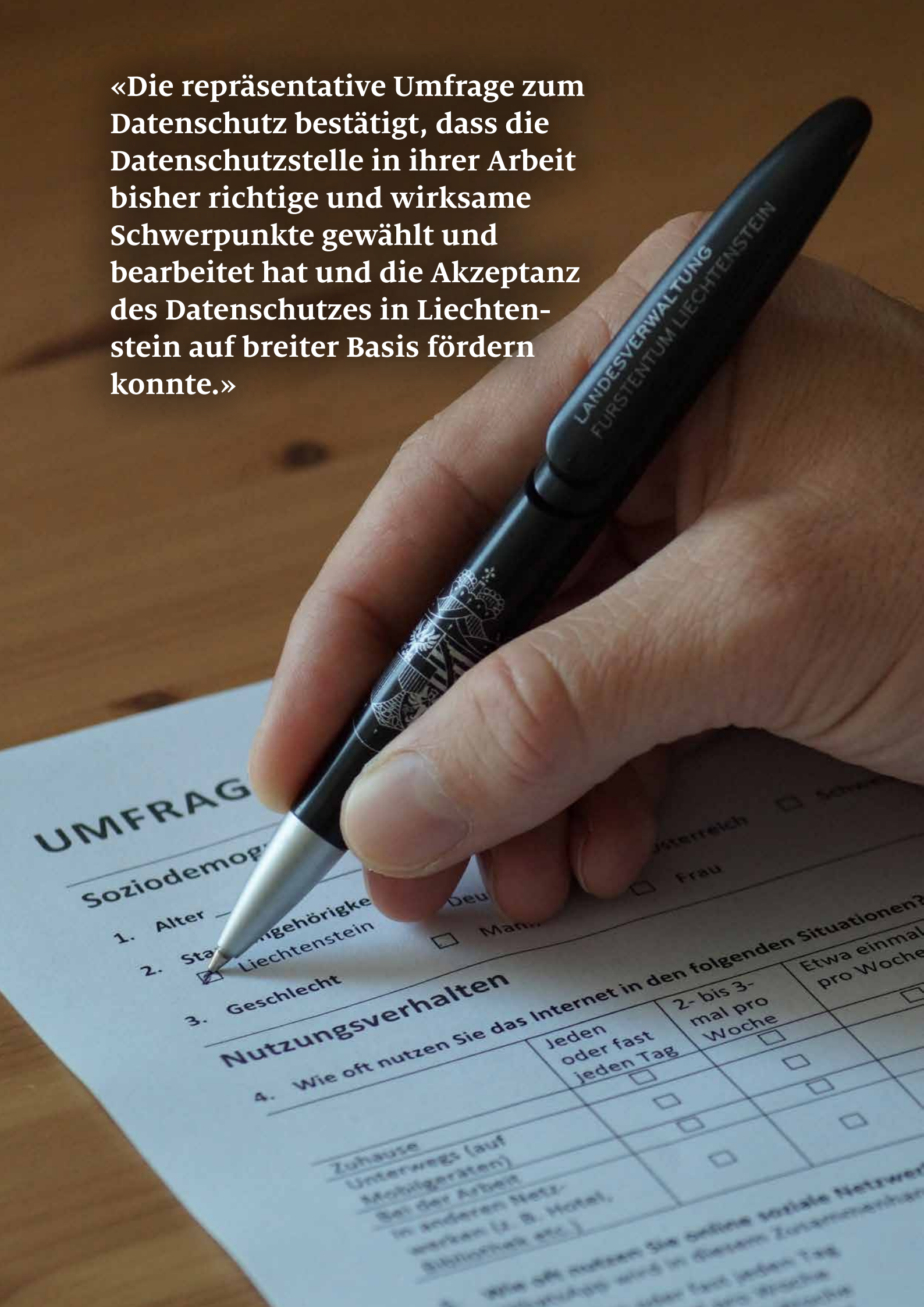
Die Datenschutzstelle betonte in ihrer Stellungnahme zum neuen E-Govenment-Gesetz, dass personenbezogene Daten gemäss DSGVO und DSG nur für festgelegte, eindeutige und legitimierte Zwecke erhoben und weiterverarbeitet werden dürfen. Aus der Festlegung der Zwecke ergibt sich auch das erforderliche Ausmass der Datenverarbeitung, auf die die Erhebung nach dem Grundsatz der Datenminimierung zu beschränken ist. Nach diesem Grundsatz dürfen Daten auch nicht auf Vorrat für mögliche künftige Zwecke erhoben werden, die zum Zeitpunkt der Erhebung noch nicht bestimmt und damit auch für die betroffenen Personen nicht vorhersehbar sind. Der Grundsatz der Speicherbegrenzung verbietet als Konkretisierung des Grundsatzes der Datenminimierung darüber hinaus, personenbezogene Daten länger zu speichern, als dies für die Zwecke ihrer Verarbeitung erforderlich ist. Aus der Regierungsvorlage liess sich nicht klar nachvollziehen, in welcher Form diese beiden Grundsätze (Datenminimierung und Speicherbegrenzung) im neuen Gesetz eingehalten und angewandt werden, weshalb von der Datenschutzstelle diesbezüglich Ergänzungen und Präzisierungen empfohlen wurden.

Abschliessend betonte die Datenschutzstelle die Wichtigkeit, die unterschiedlichen Ansätze der Regierungsvorlagen zum RVOG und zum E-Government-Gesetz miteinander in Einklang zu bringen und für die Bürgerinnen und Bürger so eine transparente, kohärente und sichere Rechtsgrundlage zu schaffen. Art. 6a des E-Government-Gesetzes stellt klar, dass ein Datenaustausch bzw. eine Wiederverwendung personenbezogener Daten ausschliesslich mit Einwilligung der betroffenen Personen zulässig ist. Wie auf Seite 18 des Vernehmlassungsberichts explizit ausgeführt wird, stehen der Austausch und die Wiederverwendung unter dem «Vorbehalt der Einwilligung der Verfahrensbeteiligten». Eine Person ist somit nicht verpflichtet, ihre behördlichen Daten für eine Weiterleitung bzw. Wiederverwendung freizugeben, wenn sie selbst das Verfahren initiiert. Eine solche Einschränkung findet sich im RVOG allerdings nicht. Aus Sicht der Datenschutzstelle und im Sinne des Grundrechtsschutzes der Bürgerinnen und Bürger ist daher eine Abstimmung zwischen den beiden geplanten Gesetzen unumgänglich.

3.3 Weitere Stellungnahmen

Darüber hinaus verfasste die Datenschutzstelle inhaltliche Stellungsnahmen zu weiteren sechs Vorlagen und Erlassen, und zwar zum Vernehmlassungsbericht der Regierung betreffend die Schaffung eines Gesetzes über das elektronische Gesundheitsdossier (EGDG), zum Vernehmlassungsbericht betreffend das Gesetz über die Abänderung des Gesetzes über den internationalen automatischen Austausch länderbezogener Berichte multinationaler Konzerne (CbC-Gesetz), zum Vernehmlassungsbericht betreffend die Abänderung des Landwirtschaftsgesetzes (LWG), zum Vernehmlassungsbericht betreffend die Abänderung des Rechtshilfegesetzes sowie des Gesetzes über das Strafregister und die Tilgung gerichtlicher Verurteilungen, zum Vernehmlassungsbericht betreffend die Schaffung eines Hypothekar- und Immobilienkreditgesetzes (HIKRG; Umsetzung Richtlinie 2014/17/EU) sowie die Abänderung weiterer Gesetze sowie zum Vernehmlassungsbericht betreffend den Erlass des EWR-Verbriefungs-Durchführungsgesetzes.

Die Prüfung von 14 weiteren Vorlagen ergab keine datenschutzrechtlichen Bedenken.



«Die repräsentative Umfrage zum Datenschutz bestätigt, dass die Datenschutzstelle in ihrer Arbeit bisher richtige und wirksame Schwerpunkte gewählt und bearbeitet hat und die Akzeptanz des Datenschutzes in Liechtenstein auf breiter Basis fördern konnte.»

4. Neuaufgaben und interne Organisation

4.1 Inkrafttreten des Datenschutzgesetzes (DSG) und der Datenschutzverordnung (DSV) am 1. Januar 2019

Das DSG vom 4. Oktober 2018 sowie die DSV vom 11. Dezember 2018 traten am 1. Januar des Berichtsjahres in Kraft. Beide Gesetzestexte verlangten von der Datenschutzstelle einiges an Arbeitsaufwand. Der Bericht und Antrag der Regierung an den Landtag betreffend die Totalrevision des Datenschutzgesetzes sowie die Abänderung weiterer Gesetze sieht an insgesamt 14 Stellen Aufgaben für die Datenschutzstelle vor, die unter anderem in der Ausarbeitung von Leitlinien zur Videoüberwachung, der Durchführung von Veranstaltungen zur Aufklärung und Sensibilisierung der Bevölkerung, dem Halten von Vorträgen, dem Erstellen von Informationsbroschüren oder der Durchführung von Öffentlichkeitskampagnen in Zeitungen und Sozialen Medien sowie auf Internetseiten bestehen. Zusätzlich sollte die Datenschutzstelle den Gemeinden in Bezug auf die Umsetzung der Datenschutzbestimmungen Hilfestellung leisten sowie die Kommunikation mit den betrieblichen und behördlichen Datenschutzbeauftragten verstärken und datenverarbeitende Stellen sowie die Öffentlichkeit über die Entscheidungen auf europäischer Ebene, welche einen grossen Einfluss auf die Anwendung der DSGVO haben, auf dem Laufenden halten. Die Datenschutzstelle nahm diese Aufgaben in ihre Planung für das Berichtsjahr auf und erfüllte sämtliche Aufgaben bis Jahresende.

Eine spezielle und herausfordernde Neuerung stellt Art. 5 DSG dar. Mit diesem Artikel wird die Videoüberwachung öffentlich zugänglicher Räume neu geregelt und insbesondere die Bewilligungspflicht durch eine Meldepflicht ersetzt. Der gleichlautende § 4 der Rezeptionsgrundlage, des deutschen Bundesdatenschutzgesetzes (BDSG-neu), stand jedoch wiederholt in der Kritik, da das Bestehen einer für seinen Erlass erforderlichen Öffnungsklausel in der DSGVO infrage gestellt wurde. Diese Problematik gilt entsprechend auch für Art. 5 DSG. Gemäss Wortlaut beschränkt sich die Öffnungsklausel des Art. 6 Abs. 2 und 3 DSGVO auf die Fälle der Datenverarbeitung nach Art. 6 Abs. 1 Bst. c und e DSGVO. Art. 5 Abs. 1 Ziff. 1 DSG («Aufgabenerfüllung öffentlicher Stellen») lässt sich somit auf Art. 6 Abs. 1 Bst. e DSGVO stützen und ist daher unbedenklich. Problematisch ist hingegen die Öffnungsklausel für die nachfolgenden Ziffern 2 und 3. Diese beiden Ziffern dürften in den Anwendungsbereich des Art. 6 Abs. 1 Bst. f DSGVO fallen, für den gerade kein Regelungsspielraum für den nationalen Gesetzgeber in Gestalt einer Öffnungsklausel besteht. Die Datenschutzstelle widmete daher dem Thema Videoüberwachung ein ausführliches Kapitel auf ihrer Internetseite und bemühte sich dabei, praktikable Lösungen vorzuschlagen, die auch dann ihre Gültigkeit behielten, sollten die Ziffern 2 und 3 im Art. 5 DSG wegfallen und für diese Arten der Videoüberwachung nur mehr Art. 6 Abs. 1 Bst. f DSGVO als Rechtsgrundlage dienen.

4.2 Umfrage zum Datenschutz 2019

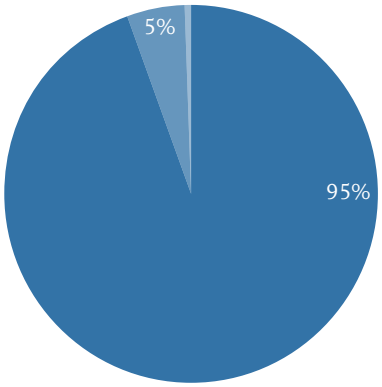
Die Datenschutzstelle hat im Spätherbst 2019 in Zusammenarbeit mit dem Liechtenstein-Institut eine repräsentative Umfrage in der Bevölkerung Liechtensteins durchgeführt, um ihre künftige Arbeit und ihre Projekte zielgerichtet planen zu können. In der Umfrage ging es deshalb insbesondere darum festzustellen, wie weit eine Sensibilisierung der Bevölkerung für den Datenschutz bereits stattgefunden hat und was ihre Einstellung dazu ist. Darüber hinaus wurde sie gefragt, wo die wichtigsten Berührungspunkte mit dem Datenschutz sind, ob die neuen rechtlichen Bestimmungen zum Datenschutz bekannt und akzeptiert sind, einschliesslich der verschiedenen Rechte für die Betroffenen, und wie weit die bisherigen Angebote der Datenschutzstelle bereits wahrgenommen oder genutzt wurden.

Die Umfrage wurde an 4'000 Personen ab 16 Jahren in Liechtenstein verschickt und war als Online-Fragebogen oder, auf Anfrage, auch als Papier-Fragebogen auszufüllen. Sie wurde von 1'219 Personen beantwortet, was einem höchst erfreulichen Rücklauf von über 30% entspricht. Die Antworten auf die im Rahmen von fünf Themenblöcken gestellten Fragen (Internetnutzung, Kenntnis von Datenschutzbestimmungen, Umgang mit Datenschutzhinweisen, Datenschutz im Allgemeinen, Datenschutz in Liechtenstein) wurden in der Folge vom Liechtenstein-Institut anonym ausgewertet. Zusätzlich wurde auch noch eine Gewichtung nach den ebenfalls erhobenen soziodemografischen Merkmalen und anderen Variablen vorgenommen (Alter, Geschlecht, Staatsangehörigkeit etc.), wobei insbesondere für das Alter über praktisch alle Fragestellungen hinweg ein signifikanter Zusammenhang festgestellt werden konnte. Wenn möglich wurde ein Vergleich zu den Ergebnissen einer im März 2019 in den EU-Mitgliedstaaten durchgeführten Umfrage, dem Special Eurobarometer 487a, hergestellt. Die Auswertung der Umfrage beschränkte sich auf eine rein beschreibende Situationsanalyse und nahm keine Erklärung etwaiger kausaler Zusammenhänge vor.

Der Blick auf die eigentlichen Umfrageergebnisse zeigt dabei zunächst, dass die Internetnutzung in Liechtenstein generell stark ausgeprägt ist: 95% der Befragten nutzen das Internet zumindest gelegentlich und 85% gar täglich. Für Einkäufe nutzen 82% der Befragten das Internet zumindest gelegentlich und 62% nutzen es für soziale Netzwerke.

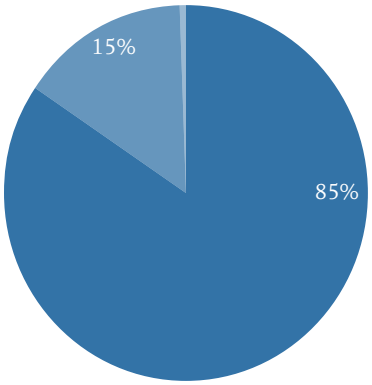
Internetnutzung in Liechtenstein

Internetnutzung in Liechtenstein



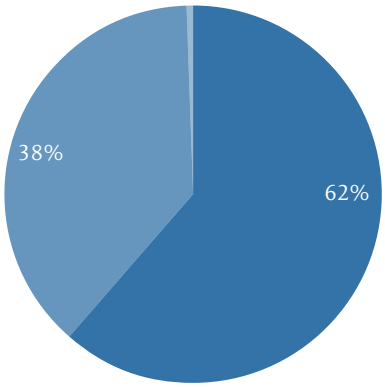
- Internetnutzung
- Keine Internetnutzung
- Weiss nicht/k. A.

Häufigkeit Internetnutzung



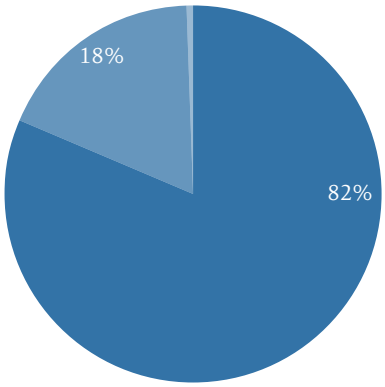
- Täglich
- Nicht täglich
- Weiss nicht/k. A.

Nutzung sozialer Netzwerke



- Soziale Netzwerke
- Keine sozialen Netzwerke
- Weiss nicht/k. A.

Internetnutzung für Einkäufe

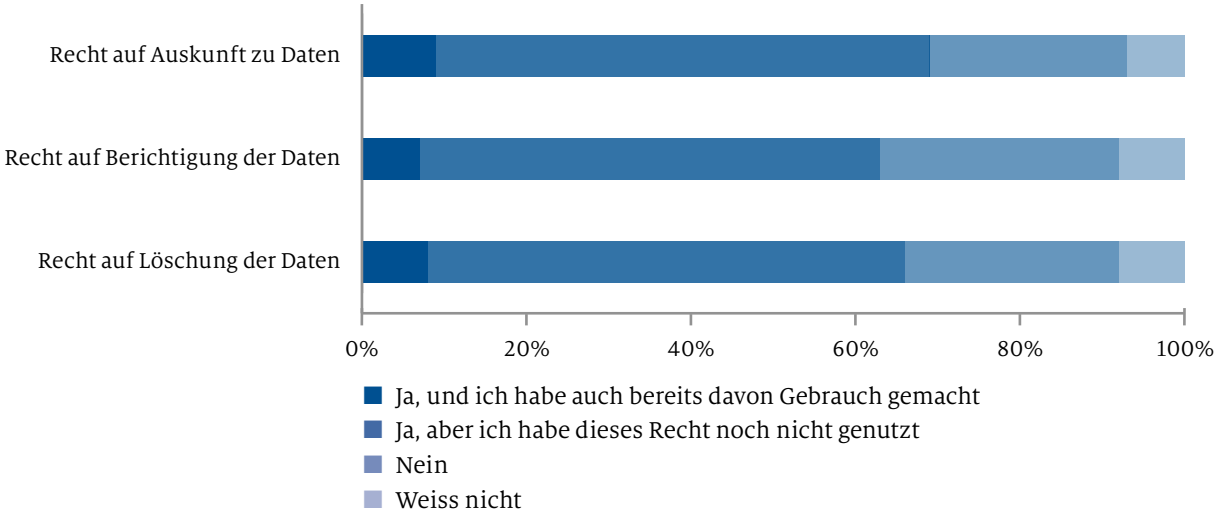


- Einkäufe im Internet
- Keine Einkäufe
- Weiss nicht/k. A.

Die Umfrage offenbarte ausserdem, dass die Bekanntheit der DSGVO mit 63% und die Kenntnis damit einhergehender Rechte für die Betroffenen mit 79% der Befragten in Liechtenstein im Vergleich zum übrigen Europa relativ hoch sind. Ungeachtet dessen haben die Menschen in Liechtenstein bisher noch nicht sehr oft von diesen Rechten Gebrauch gemacht.

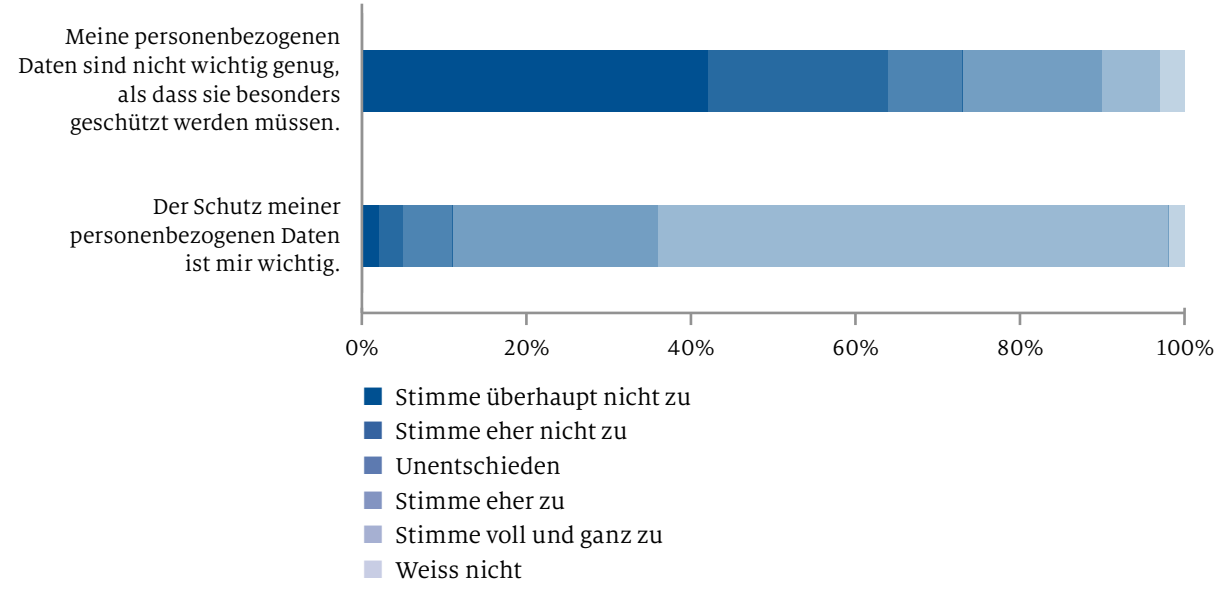
Datenschutzhinweise im Internet werden von rund der Hälfte der Befragten zumindest teilweise gelesen. Lediglich 25% geben jedoch an, dass sie diese Hinweise auch meistens verstehen.

Kenntnisse über einzelne Datenschutz-Rechte



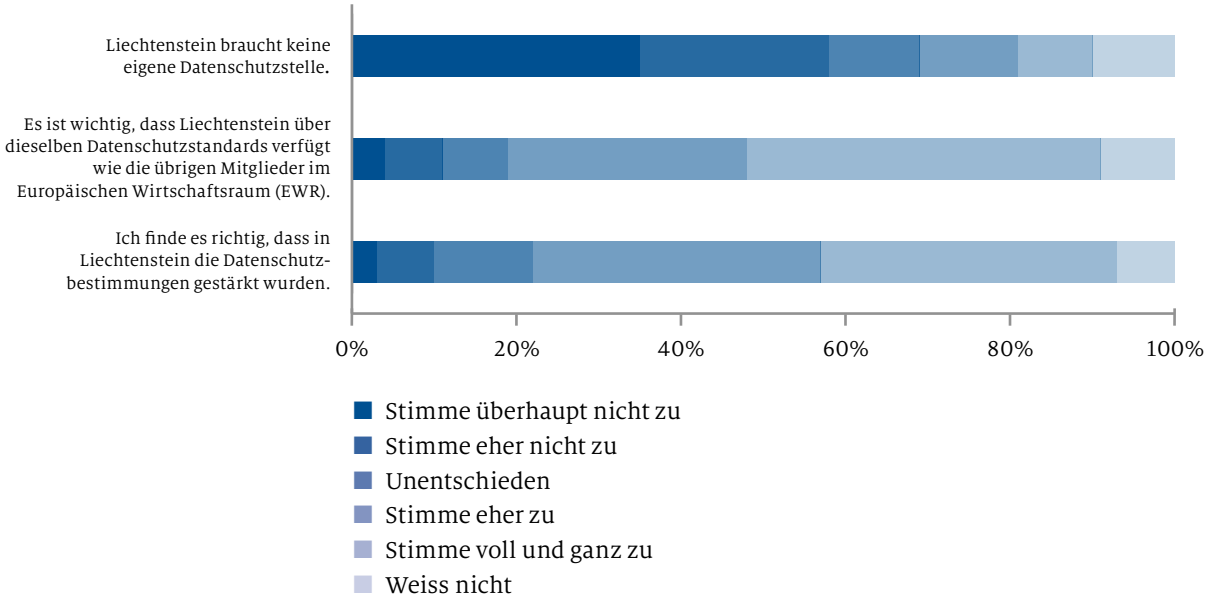
Die grosse Mehrheit der befragten Personen in Liechtenstein sagt, dass ihr der Schutz ihrer personenbezogenen Daten grundsätzlich wichtig ist (87%). Es glauben jedoch nur gerade 5% der Befragten, dass sie die volle Kontrolle über online zur Verfügung gestellte Informationen besitzen. Tatsächlich Sorgen bereitet diese mangelnde Kontrolle aber wiederum nur knapp der Hälfte der befragten Personen.

Allgemeine Einstellung zum Schutz personenbezogener Daten



Fast 60% der Befragten haben schon vor der Umfrage einmal von der Datenschutzstelle gehört und einige haben auch bereits Veranstaltungen der Datenschutzstelle oder die Internetseite der Datenschutzstelle besucht. Eine deutliche Mehrheit der befragten Personen ist der Meinung, dass die Datenschutzbestimmungen in Liechtenstein zu Recht gestärkt (71%) und den Datenschutzstandards wie in den anderen EWR-Ländern angepasst wurden (72%). Der Datenschutz und die Datenschutzstelle sehen sich damit – trotz des verbreitet wahrgenommenen angestiegenen, bürokratischen Aufwands und einigen Zweifeln an der Wirksamkeit der Bestimmungen – grundsätzlich einer hohen Akzeptanz in Liechtenstein gegenüber.

Einschätzung der Datenschutzregulierung in Liechtenstein



Für die Arbeit der Datenschutzstelle bedeutet dies, dass sie bisher grundsätzlich richtige und wirksame Schwerpunkte gewählt und bearbeitet hat und die Akzeptanz des Datenschutzes in Liechtenstein auf breiter Basis fördern konnte. Angesichts der Tatsache, dass erst 6% der Befragten in der Vergangenheit schon eine Veranstaltung der Datenschutzstelle besucht haben, gilt es künftig insbesondere in diesem Bereich das Angebot der Datenschutzstelle noch zu verbreitern und vielfältiger zu gestalten, um weitere Zielgruppen zu erreichen. Im vergangenen wie auch im laufenden Jahr stehen dabei speziell Eltern und Schüler und Schülerinnen bzw. Jugendliche im Fokus. Auch andere Zielgruppen werden indes nicht vergessen. So ist für 2020 beispielsweise eine Veranstaltung für Senioren geplant, bei der die Datenschutzstelle wesentliche Inhalte mitgestalten wird.

Die vollständige Studie zur Umfrage mit allen Ergebnissen und Auswertungen ist beim Liechtenstein-Institut oder bei der Datenschutzstelle erhältlich.

4.3 Personal

Am 3. Juli 2018 stellte die Datenschutzstelle in Absprache mit der Regierung beim Landtag einen Antrag auf Genehmigung von 3.5 zusätzlichen Stellen, um die neuen Aufgaben bewältigen zu können. Von den beantragten 3.5 Stellen wurden 2.5 Stellen ab 1. Januar 2019 genehmigt. Im Dezember 2018 erfolgte die Ausschreibung für diese Stellen, das heisst konkret für zwei Juristinnen bzw. Juristen sowie eine Informatikerin bzw. einen Informatiker. Im Laufe des Berichtsjahres konnten die offenen Stellen besetzt werden. Dies erlaubte es der Datenschutzstelle, die vor allem qualitativ gestiegenen Anforderungen in der Beratung weiterhin zu bewältigen. Daneben konnten eigene Projekte insbesondere im Bereich Datenschutz und Kinder/Jugendliche in Angriff genommen sowie die Beratung und Bearbeitung von Beschwerden im Bereich Videoüberwachung gewährleistet werden. Die personelle Verstärkung der Datenschutzstelle erlaubte es ihr ausserdem im Bereich Blockchain tätig zu werden, die Arbeit in Bezug auf die Beteiligung am Schengen-Raum wieder aufzunehmen und aktiver auf Ebene des Europäischen Datenschutzausschusses sowie des Europarates tätig zu sein.

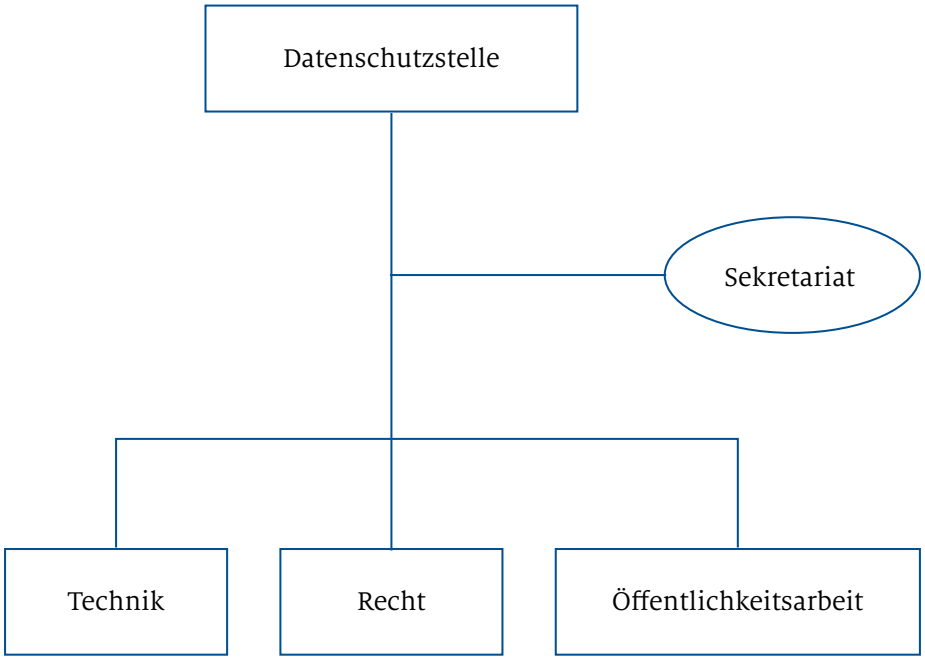


Abbildung 3: Organigramm Datenschutzstelle

«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 nicht allein auf die Eigenverantwortung der Verantwortlichen und Auftragsverarbeiter, sondern erachtet darüber hinaus die Aufsicht der Datenschutzaufsichtsbehörden als unabdingbar. Gemäss Art. 57 Abs. 1 Bst. a DSGVO *muss* die Aufsichtsbehörde die Anwendung dieser Verordnung überwachen. Dazu soll die Behörde nach Bst. h «*Untersuchungen über die Anwendung dieser Verordnung durchführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde*». Im Rahmen einer solchen Untersuchung stehen der Aufsichtsbehörde alle in Art. 58 Abs. 1 DSGVO genannten Untersuchungsbefugnisse zur Verfügung.

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

Wie im Tätigkeitsbericht 2018 angekündigt, begann die Datenschutzstelle im Herbst des Berichtsjahres mit der amtswegigen Durchführung von Datenschutzüberprüfungen. Dazu wurden für einen ersten Durchgang zehn mittelständische Unternehmen nach dem Zufallsprinzip ausgewählt. Diese Unternehmen erhielten einen Fragebogen, mit dem überprüft wurde, inwieweit die Verantwortlichen die gesetzlichen Vorgaben aus der DSGVO in verschiedensten Bereichen (Gesetzliche Grundlagen der personenbezogenen Datenverarbeitung, Führung des Verzeichnisses der Verarbeitungstätigkeiten, Informationspflichten gegenüber den Betroffenen, Umsetzung der Betroffenenrechte, Datensicherheit, Auftragsverarbeitungsverträge, technische und organisatorische Massnahmen etc.) erfüllt haben. Da die Verantwortlichen zu diesem Zeitpunkt bereits mehrere Jahre Zeit zur Verfügung hatten, diese verpflichtenden Vorgaben umzusetzen, war von der Datenschutzstelle erwartet worden, dass dieser sehr allgemein gehaltene Prüfungsdurchgang für die Unternehmen keine allzu grosse Hürde darstellen dürfte. Erste Ergebnisse zeigten, dass sechs Unternehmen eine sehr gute bis gute Umsetzung aufwiesen, während bei vier Unternehmen die Umsetzung als ausreichend bis mangelhaft beurteilt werden musste. Bei den mangelhaft bewerteten Unternehmen waren entsprechende Anpassungen beziehungsweise Ergänzungen notwendig.

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 Datenschutzstelle – wie in Erwägungsgrund 141 der DSGVO empfohlen – auf der Internetseite im Abschnitt *Services* ein elektronisches Beschwerdeformular an.

Im Berichtsjahr erhielt die Datenschutzstelle 41 Beschwerden, die sich gegen einen Verantwortlichen in Liechtenstein richteten. 13 dieser Beschwerden wurden von Personen im Ausland eingebracht. 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 Datenschutzstelle etwa 10% unter der Anzahl des Vorjahres.

In 29 Beschwerdefällen konnte mit der datenverarbeitenden Stelle eine einvernehmliche Lösung gefunden werden, worauf die Beschwerden zurückgezogen und eine gütliche Einigung erreicht wurde. Mit diesem auch in Erwägungsgrund 131 der DSGVO empfohlenen Vorgehen konnten im Berichtsjahr zahlreiche langwierige und aufwändige Verfahren verhindert werden.

Zwölf Beschwerden wurden mit einer Verfügung entschieden, wobei die Datenschutzstelle von ihren Befugnissen unter Art. 58 Abs. 2 DSGVO weitreichend Gebrauch machte und Verwarnungen, Anweisungen, Beschränkungen und Verbote aussprach. Geldbussen wurden hingegen im Berichtsjahr keine verhängt.

Die im Berichtsjahr erlassenen Verfügungen bzw. Berichte befassten sich unter anderem mit folgenden Fragen:

Kann der Beschwerdeführer von der Datenschutzstelle verlangen, gegen den Verantwortlichen eine bestimmte Abhilfemassnahme zu ergreifen, insbesondere eine Geldbusse zu verhängen?

Art. 77 DSGVO gewährt jeder betroffenen Person ein Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstösst. Die Behörde hat die Beschwerde mit aller gebotenen Sorgfalt und in angemessenem Umfang zu prüfen. Der Beschwerdeführer hat allerdings keinen Anspruch darauf, dass die Behörde bestimmte, von ihm geforderte Massnahmen ergreift. Die Behörde ist einzig verpflichtet, bei festgestellten Verstössen alle Massnahmen zu ergreifen, die für die Abstellung des Verstosses als erforderlich erachtet werden. Dazu können, müssen aber nicht, auch Geldbussen in Frage kommen. Eingeschränkt wird die Verhängung von Geldbussen zudem durch Art. 40 Abs. 6 DSG, der besagt: *«Die Datenschutzstelle wird den Katalog des Art. 83 Abs. 2 bis 6 der Verordnung (EU) 2016/679 so zur Anwendung bringen, dass die Verhältnismässigkeit gewahrt wird. Insbesondere bei erstmaligen Verstössen wird die Datenschutzstelle im Einklang mit Art. 58 der Verordnung (EU) 2016/679 von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen.»*

Die Datenschutzstelle sah im konkreten Fall unter Zugrundelegung von Art. 40 Abs. 6 DSG sowie der in Art. 83 Abs. 2 DSGVO genannten Kriterien eine Geldbusse nicht als erforderlich an, sondern erachtete die gemäss Spruch getroffenen Massnahmen als angemessen und ausreichend, um eine Abstellung des Verstosses zu bewirken.

Ist die Weitergabe von zwei ausgedruckten Fotos einer dritten Person mit dem Auftrag, diese an bestimmter Stelle zu hinterlegen, als widerrechtliche Datenverarbeitung zu qualifizieren, wenn dafür kein Rechtfertigungsgrund im Sinne des Art. 6 DSGVO vorliegt?

Bei Fotos in Papierform handelt es sich zwar grundsätzlich um personenbezogene Daten, nämlich Bilddaten, allerdings wurden diese Bilddaten im konkreten Fall durch die Weitergabe nicht einer ganz oder teilweise automatisierten Verarbeitung zugeführt. Dazu müsste eine Datenverarbeitungsanlage zum Einsatz kommen. Dies ist durch die manuelle Entgegennahme von zwei Fotos und deren manuellen Einwurf in einen Briefkasten nicht erfüllt. Somit bleibt nur der zweite Anwendungsbereich des Art. 2 Abs. 1 DSGVO zu prüfen: die nichtautomatisierte Verarbeitung personenbezogener Daten. Darunter versteht Erwägungsgrund 15 der DSGVO die manuelle Verarbeitung von personenbezogenen Daten. Voraussetzung ist allerdings, dass die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Art. 4 Ziff. 6 DSGVO versteht unter Dateisystem *«jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird»*.

Im konkreten Fall war bei der manuellen Entgegennahme und Weitergabe der ausgedruckten Fotos keine Ordnung nach bestimmten Kriterien erkennbar. Es handelte sich folglich um eine rein manuelle Verarbeitung personenbezogener Daten ohne strukturiertes Dateisystem. Aus diesem Grund war der sachliche Anwendungsbereich im Sinne von Art. 2 Abs. 1 DSGVO nicht eröffnet, weshalb die Beschwerde in diesem Punkt abzuweisen war.

Ist die Nennung des Namens und der Privatadresse einer Person, die durch Landtagsentscheid in ein öffentliches Amt berufen wurde, im öffentlich zugänglichen Sitzungsprotokoll zulässig?

Eine Prüfung der entsprechenden Protokolle und Berichte ebenso wie der Rechtsgrundlagen für die Veröffentlichung der Namen und der Privatadressen ergab, dass die Veröffentlichung des *Namens* gemäss Art. 6 Abs. 1 Bst. e DSGVO im konkreten Fall gerechtfertigt war. Hingegen konnte von der Datenschutzstelle kein Rechtfertigungsgrund identifiziert werden, der die Nennung der *Privatadresse* in einem öffentlich (sprich über das Internet) zugänglichen Dokument vorschreibt. Gemäss Art. 5 DSGVO ist die Datenminimierung ein wesentlicher Grundsatz einer jeglichen Datenverarbeitung und es dürfen daher nur jene Daten verarbeitet (und im konkreten Fall publiziert) werden, die zur Erreichung eines bestimmten Zweckes erforderlich sind. Wenn man davon ausgeht, dass der Zweck der Berichte und Protokolle des Landtags die Information der Öffentlichkeit ist, dann wäre aus Sicht der Datenschutzstelle der Zweck auch dann erreicht, wenn darin jeweils nur der Name der in ein öffentliches Amt berufenen Person aufscheint und auf die Privatadresse verzichtet wird. Denn diese bringt keinen Mehrwert für die Information der Öffentlichkeit bzw. die Transparenz des Landtages.

Ist das Double-Opt-in-Verfahren bei Newslettern als ein Verfahren zu qualifizieren, das gewährleistet, dass eine Einwilligung im Sinne von Art. 7 DSGVO rechtskonform eingeholt wird?

Im konkreten Fall ging es um eine in ein Double-Opt-In-Verfahren eingebettete Einwilligungserklärung einer betroffenen Person, mittels welcher diese zugestimmt hatte, von einem Unternehmen postalisch oder per E-Mail über Angebote informiert zu werden. Es war im fraglichen Verfahren aber möglich gewesen, auch mit

einer gefälschten E-Mail-Adresse dem Versand an eine Post-Adresse zuzustimmen. Die Person, welche die Einwilligung mittels gefälschter E-Mail-Adresse abgab, war somit in vielen Fällen vom tatsächlichen Empfänger der postalischen Werbung verschieden. Aufgrund des offenkundigen Bekanntseins dieser Manipulationsmöglichkeit sah die Datenschutzstelle die Einwilligung im konkreten Fall nicht als rechtskonform an und stellte fest, dass die Beschwerdegegnerin zusätzliche Massnahmen gemäss Art. 32 DSGVO implementieren müsse, um das Double-Opt-In-Verfahren gegen solche Manipulationen durch Unbefugte und somit eine widerrechtliche Datenverarbeitung zu schützen.

Ist es zulässig, eine Einwilligung in die Weitergabe personenbezogener Daten an Dritte auch auf solche Dritte (Unternehmen) zu beziehen, die nicht in der Einwilligungserklärung selbst, sondern in den Allgemeinen Geschäftsbedingungen bzw. anderen Erklärungen genannt werden?
Eine rechtsgültige Einwilligung hat unter anderem gemäss Art. 7 DSGVO stets in informierter Weise zu erfolgen. Dem Grundsatz der Informiertheit entsprechend muss eine einwilligende Person eindeutig abschätzen können, welche Auswirkungen die Erteilung einer Einwilligung für sie hat, und sie muss die Umstände der Datenverarbeitung eindeutig erkennen können.

Im konkreten Fall wurde die betroffene Person gemäss Einwilligungstext darüber informiert, dass sie von einem bestimmten Unternehmen und den in der anschliessenden Auflistung ausgewiesenen Partnerunternehmen postalisch oder per E-Mail über Angebote informiert werden kann. In den Datenschutzbestimmungen wurde jedoch ausgeführt, dass zusätzlich «beauftragte Dienstleister» die Daten für Marktforschung, für die bessere Zuordnung von bereits zu der betroffenen Person vorhandenen Daten sowie für interessante und günstige Werbeangebote, die den erkennbaren Interessen entgegenkommen, verarbeiten und nutzen dürfen. Damit waren die möglichen Datenverarbeitungen sowie der Kreis der Datenempfänger aber deutlich umfassender als in der eigentlichen Einwilligungserklärung angegeben. Der Einwilligung fehlte somit als wesentliches Kernelement die Informiertheit und sie war folglich mangelhaft und damit ungültig.

Ist die Aufzeichnung von Telefongesprächen zu Beweiszwecken zulässig?
Die bei Banken gesetzlich verankerte Obliegenheit der Aufzeichnung von Kundentelefonaten in bestimmten Kontexten liess offensichtlich auch bei anderen Wirtschaftsakteuren den Wunsch der Aufzeichnung von Kundentelefonaten entstehen. Gestützt auf Art. 16 MIFID II sind Banken gesetzlich zur Aufzeichnung von Telefongesprächen, die sich auf die Annahme, Übermittlung und Ausführung von Kundenaufträgen beziehen, gehalten. Ausserhalb der von MIFID II angesprochenen Institutionen freilich kann MIFID II nicht als Rechtsgrundlage für die Aufzeichnung von Telefonaten dienen. Andere Wirtschaftsakteure haben dafür dementsprechend nach anderen Rechtfertigungsgründen zu suchen. Gemäss Art. 6 Abs. 1 DSGVO sind mögliche Rechtfertigungsgründe für die Datenverarbeitung neben einem Gesetz insbesondere ein Vertrag, die Einwilligung oder in sehr engen Grenzen das berechtigte Interesse. Im Kontext von Telefongesprächen ist – abgesehen von der Einhaltung gesetzlicher Bestimmungen insbesondere im Finanzsektor – in aller Regel die Einwilligung Rechtfertigungsgrund für die Aufzeichnung von Telefonaten mit externen Gesprächspartnern. Nicht korrekt umgesetzt ist die Einwilligung, wenn sie als ein simples Widerspruchsrecht (Opt-Out) ausgestaltet ist. Gemäss Art. 4 Ziff. 11 DSGVO muss die Einwilligung durch die betroffene Person in Form einer Erklärung oder einer sonstigen bestätigenden Handlung eindeutig erfolgen (Opt-In). Soll die Telefonaufzeichnung den Erfordernissen der Einwilligung gemäss Art. 4 Ziff. 11 DSGVO genügen und damit erlaubt sein, wäre die betroffene Person vor Beginn der beabsichtigten Telefonaufzeichnung zu fragen, ob sie mit der Aufzeichnung des Telefonats einverstanden ist, und müsste sie bejahendenfalls ihr Einverständnis durch eine aktive bestätigende Handlung, wie Aussprechen eines «Ja» oder der Betätigung einer bestimmten Telefontaste, eindeutig geben.

In Bezug auf Videoüberwachungen erreichten eine Vielzahl von formellen und informellen Beschwerden die Datenschutzstelle. Waren es in anderen Jahren mit Kamera bestückte Drohnen, die für rauchende Köpfe in der Bevölkerung wie auch in der Datenschutzstelle sorgten, so waren es im Berichtsjahr vor allem Videoüberwachungen im Nachbarschaftsbereich. Drei formelle Beschwerden wurden dazu bei der Datenschutzstelle eingereicht. Bei zweien ging es um fest installierte Videokameras und dem Verdacht, dass von den Linsen jeweils mehr erfasst würde als nur das private Grundstück des Betreibers. In beiden Fällen hat die Datenschutzstelle den Kontakt zu den Betreibern gesucht, um die Sachlage zu klären und eine entsprechende Verfügung erlassen zu können. Darin hielt die Datenschutzstelle unter anderem fest, dass es unzulässig ist, mit einer Videokamera eine private Zufahrtsstrasse komplett zu erfassen, wenn diese auch von anderen Anrainern genützt wird.

Neben den formellen Beschwerden erreichten die Datenschutzstelle im Berichtsjahr auch vier informelle Beschwerden bezüglich Videoüberwachungen in nachbarschaftlichen Verhältnissen. Zu diesen hat die Datenschutzstelle jeweils vor Ort oder telefonisch Rat erteilt, oder blieb – auf Wunsch – auch gänzlich im Hintergrund, um ein behördliches Auftreten zu vermeiden. Bei diesen Beschwerden bestand häufig Unklarheit darüber, dass auch Videoüberwachungen auf Privatgrundstücken grundsätzlich der DSGVO unterliegen und somit deren rechtliche Voraussetzungen, wie etwa die Informationspflicht, einzuhalten sind. Eine weitere informelle Beschwerde betraf die Videoüberwachungsanlage eines Fitnessstudios, welche den Trainingsbereich erfasste. Sie war grundsätzlich unzulässig, da es sich beim erfassten Bereich um einen Ort zur Freizeitgestaltung handelte.

Die vielen Beschwerden formeller und informeller Art zu Videoüberwachungen im Nachbarschaftsbereich haben die Datenschutzstelle bewogen, ihre Informationen dazu auf der Internetseite weiter auszubauen. Um den Dialog unter den beteiligten Nachbarn zu fördern und eine Eskalation der Streitigkeit möglichst zu vermeiden, hat die Datenschutzstelle auch ein Informationsschreiben entworfen, welches Personen, die sich durch Videoüberwachungskameras ihrer Nachbarn gestört fühlen, diesen anonym oder unterzeichnet in den Briefkasten legen können. Das Schreiben informiert über die generellen Grundbedingungen der Zulässigkeit von Videokameras.

5.2.1 Beschwerden an die Beschwerdekommission für Verwaltungsangelegenheiten

In vier Beschwerdefällen erhob der Beschwerdegegner Beschwerde an die Beschwerdekommission für Verwaltungsangelegenheiten. Diese wiederum legte in zwei Fällen zwei Rechtsfragen dem EFTA-Gerichtshof vor, der sie in der Folge miteinander verband. In diesem Verfahren ist eine Entscheidung voraussichtlich nicht vor Ende 2020 zu erwarten.

5.3 Meldung von Datenschutzverletzungen gemäss Art. 33 DSGVO

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

Im Berichtsjahr erhielt die Datenschutzstelle 16 Meldungen von Datenschutzverletzungen nach Artikel 33 DSGVO, wovon in einem Fall auch eine Information der Betroffenen nach Artikel 34 DSGVO zu erfolgen hatte. Die Meldungen zeigten, dass es für die Verantwortlichen nicht immer einfach war, innerhalb der 72-Stunden-Frist alle relevanten Informationen im Unternehmen zusammenzutragen und beizubringen. Vielfach mussten daher fehlende Informationen in einem weiteren Schritt zu einem späteren Zeitpunkt nachgeliefert werden.

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 Datenschutzstelle unterstützte die Verantwortlichen deshalb bei der Klärung dieser Frage. Nur in einem Fall ergab sich letztlich die Notwendigkeit zur Information der Betroffenen.

Ein weiterer Fall, in dem die Datenschutzstelle bezüglich der Information der Betroffenen beratend tätig war, betraf keine liechtensteinische Meldung einer Datenschutzverletzung an die Datenschutzstelle, sondern eine grössere Datenschutzverletzung im Juli 2019 bei der bulgarischen Steuerbehörde. Dabei wurden zwar insbesondere Daten bulgarischer Steuerzahler, aber eben vereinzelt auch im Rahmen des automatischen Informationsaustauschs (AIA) an Bulgarien übermittelte Steuerdaten aus anderen Ländern offengelegt. Die Datenschutzstelle begleitete die liechtensteinische Steuerverwaltung in der Einschätzung der Lage und des weiteren Vorgehens in Bezug auf die Erfüllung datenschutzrechtlicher Informationspflichten an betroffene Personen in Liechtenstein.

«Die Unterstützung der Landesverwaltung in Zusammenarbeit mit der behördlichen Datenschutzbeauftragten bildete im Berichtsjahr einen wichtigen Aspekt der Arbeit der Datenschutzstelle.»

6. Mitarbeit in Arbeitsgruppen und Projekten der Landesverwaltung

6.1 Projekt Elternportal (cse.kibe)

Im vergangenen Jahr wurde die Datenschutzstelle mehrfach zu Rate gezogen vom Ministerium für Gesellschaft, vom Amt für Soziale Dienste und vom Amt für Informatik bezüglich datenschutzrechtlicher Aspekte bei der Einführung einer zentralen Abrechnungsplattform für staatlich subventionierte Kinderbetreuungseinrichtungen. Die Datenschutzstelle unterstützte dabei einerseits die Ausgestaltung der Internetseite und der Datenbank in Bezug auf eine Begrenzung der Datenverarbeitung auf das absolut erforderliche Mass sowie in Bezug auf die Zuweisung der (begrenzten) Benutzerrechte. Andererseits begleitete die Datenschutzstelle die Ausarbeitung eines adäquaten Auftragsverarbeitungsvertrags mit dem Schweizer Dienstleister, die Entwicklung einer umfassenden Datenschutzinformation für die betroffenen Eltern auf dem so genannten Elternportal, sowie die Gewährleistung eines hohen Niveaus an Datensicherheit auf der entwickelten Internetseite und Datenbank. Auch mit den betroffenen Kinderbetreuungseinrichtungen wurde an umfassenden und zugleich leicht verständlichen Datenschutzinformationen für die Eltern wie auch für das Betreuungspersonal gearbeitet, die jenen Teil der Datenverarbeitung betreffen, der nach wie vor direkt vor Ort in den Kinderbetreuungseinrichtungen stattfindet.

6.2 Blockchain im Kontext der DSGVO

Am 1. Januar 2020 ist in Liechtenstein das Token- und VT-Dienstleister-Gesetz (TVTG) in Kraft getreten. Dieses Gesetz legt den Rechtsrahmen für Transaktionssysteme, die auf vertrauenswürdigen Technologien beruhen, fest. Blockchain-basierte Systeme stellen Ausprägungen solcher vertrauenswürdigen Technologien dar. Insbesondere im Zusammenhang mit der seit 20. Juli 2018 in Liechtenstein unmittelbar wirksamen DSGVO stellen sich zahlreiche Fragen hinsichtlich ihrer Vereinbarkeit mit dem Einsatz vertrauenswürdiger Technologien. Je nach konkreter Ausgestaltung einer Blockchain bzw. eines VT-Systems sind Fragen bezüglich der Bestimmung der Verantwortlichen, der Qualifizierung von personenbezogenen Daten im Zusammenhang mit kryptographischen Elementen oder der Wahrung von Betroffenenrechten zu klären. Des Weiteren können Spannungen in Bezug auf die Grundsätze der Verarbeitung personenbezogener Daten gemäss Art. 5 DSGVO auftreten. Die Einhaltung des Grundsatzes der Datenminimierung oder die Notwendigkeit, Daten jederzeit berichtigen bzw. löschen zu können, seien hier beispielhaft erwähnt.

Angesichts dieser Vielzahl an offenen Fragen gelangte die Stabstelle für Finanzplatzinnovation (SFI) an die Datenschutzstelle mit dem Vorschlag, ein gemeinsames Positionspapier auszuarbeiten. In diesem sollten Spannungsfelder aufgezeigt und anhand konkreter Anwendungsbeispiele Lösungskonzepte erarbeitet werden. Erste Ideen für Anwendungsbeispiele, abseits der klassischen Kryptowährungen, wurden im November 2019 von der SFI eingebracht. Diese Beispiele stellten sich jedoch als zu generisch heraus, als dass eine konkrete Beschreibung und Bewertung des Sachverhaltes aus datenschutzrechtlicher Sicht bisher möglich gewesen wäre. Die Datenschutzstelle bleibt sowohl mit der SFI als auch der Finanzmarktaufsicht (FMA) in Kontakt, damit aufgrund aktueller Entwicklungen im VT-Umfeld das Positionspapier so bald wie möglich entsprechend weiterentwickelt werden kann.

6.3 Zentrale Stammdaten

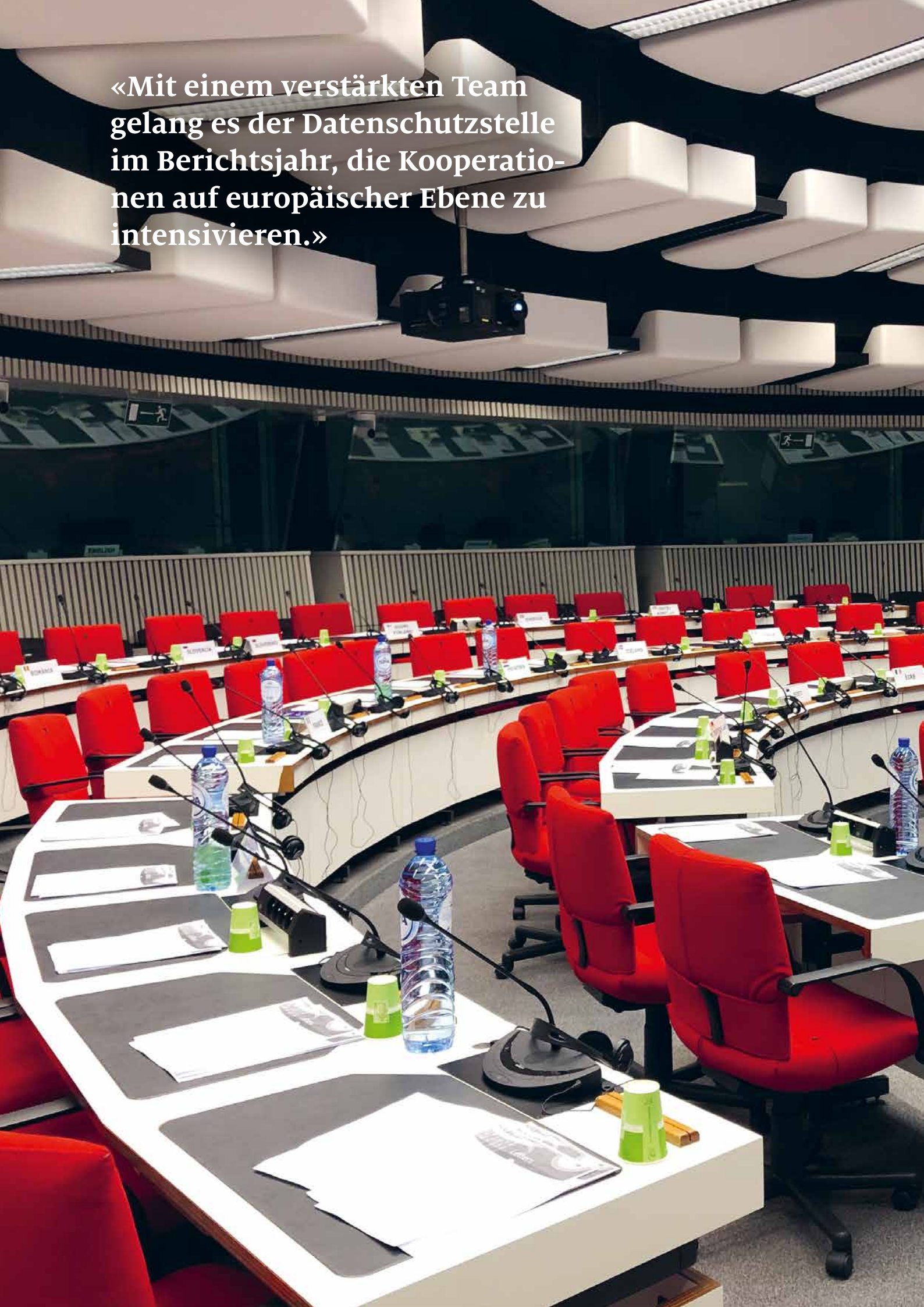
Das Zentrale Personenregister (ZPR) wurde Ende der Neunzigerjahre in der Landesverwaltung eingeführt und seither laufend ausgebaut. Die zentral geführte Datenbank wird von zahlreichen Amtsstellen genutzt und enthält unter anderem Daten sämtlicher Einwohner Liechtensteins und Daten von im Ausland wohnhaften Personen, die mit der Landesverwaltung in Kontakt getreten sind. Sie stellt daher ein besonders wichtiges Arbeitsinstrument der Landesverwaltung dar. Aus verschiedensten Gründen wurden bereits 2017 seitens der Regierung erste Aufgabenpakete für eine Modernisierung des ZPR beschlossen. Die Datenschutzstelle war darüber von Beginn an informiert und wurde seitens des Amts für Informatik regelmässig über den Projektfortschritt unterrichtet.

Im Berichtsjahr fanden im Zusammenhang mit der Modernisierung des ZPR mehrere Treffen mit der Projektleitung beim Amt für Informatik statt, an denen die Entwicklungen im Bereich Datenschutz und deren Auswirkungen auf das Projekt besprochen wurden. Unter anderem wurde dabei festgestellt, dass insbesondere aufgrund der mit der Art, dem Umfang und den Zwecken der Datenverarbeitung im modernisierten ZPR verbundenen hohen Risiken für die Rechte und Freiheiten natürlicher Personen eine Datenschutz-Folgenabschätzung gemäss Art. 35 DSGVO durchzuführen ist. Keine Einigkeit zwischen der Projektleitung und der Datenschutzstelle konnte im

Zusammenhang mit der datenschutzkonformen Ausgestaltung des künftigen Berechtigungskonzepts im weitesten Sinn sowie dem Zugriff durch Mitarbeitende der Landesverwaltung auf gespeicherte historische Daten gefunden werden. Betreffend diese Punkte kündigte das Amt für Informatik schliesslich an, in alleiniger Zusammenarbeit mit der Fachstelle Datenschutz der Landesverwaltung mögliche Lösungen evaluieren und die Zugriffe auf das modernisierte ZPR datenschutzkonform ausgestalten zu wollen. Neben technischen Aspekten, die bei der Neugestaltung des ZPR in Bezug auf den Datenschutz zu berücksichtigen sind, stellten sich auch zahlreiche rechtliche Fragen bei der (Total-)Revision des Gesetzes über das Zentrale Personenregister (ZPRG). Die Datenschutzstelle unterstützte die Regierung bei der Schaffung der entsprechenden Rechtsgrundlagen durch Stellungnahmen und die Beantwortung konkreter Fragestellungen.

6.4 Datenschutz-Folgenabschätzungen

Sämtliche Amtsstellen der Landesverwaltung werden in Angelegenheiten betreffend das Business Services Management durch sogenannte Business Consultants beim Amt für Informatik (AI) aktiv betreut. Die Business Consultants unterstützen dabei die Amtsstellen durch Beratung über die Planung und die Implementierung von Anforderungen bis zur Übergabe von IT-Lösungen in den Betrieb. Seit Inkrafttreten der DSGVO muss unter bestimmten Umständen bei Datenverarbeitungen vorgängig eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden. Dabei sind gemäss Art. 35 Abs. 1 DSGVO insbesondere die Art, der Umfang, die Umstände und der Zweck der Datenverarbeitung zu berücksichtigen. Um die Business Consultants im Umgang mit dieser Thematik zu schulen, führte das AI in Kooperation mit der Datenschutzstelle an zwei Terminen interne Workshops zum Thema durch. Die Workshops dauerten jeweils einen halben Tag und beinhalteten einen einleitenden Theorieteil sowie einen anschliessenden praktischen Teil, bei dem die Teilnehmenden anhand eines konkreten Sachverhalts eine DSFA durchführten. Im Zuge der Vorbereitung des Workshops entstand auch eine äusserst nützliche Checkliste, die es den Business Consultants in einfacher Weise erlaubt, durch die Beantwortung einiger weniger Fragen festzustellen, ob im konkreten Fall eine DSFA durchzuführen ist.



«Mit einem verstärkten Team gelang es der Datenschutzstelle im Berichtsjahr, die Kooperationen auf europäischer Ebene zu intensivieren.»

7. Internationale Zusammenarbeit

7.1 Europäischer Datenschutzausschuss (EDSA)

Eine der Hauptaufgaben des EDSA ist der Erlass von Leitlinien, die der Auslegung der DSGVO dienen. Die Grundlagen für die Leitlinien des Ausschusses werden in insgesamt zwölf thematischen Arbeitsgruppen *(expert subgroups)* geschaffen, welche die Dokumente für die Abstimmung im Ausschuss vorbereiten. Aufgrund der personellen Situation war es der Datenschutzstelle allerdings auch im Berichtsjahr nicht möglich, an den Sitzungen sämtlicher Arbeitsgruppen teilzunehmen oder zu allen Entwürfen Stellung zu nehmen. Es wurde daher eine – vielfach telefonische – Teilnahme in jenen Arbeitsgruppen beschlossen, in denen die Mitarbeitenden der Datenschutzstelle das meiste Know-how einbringen konnten oder deren Aufgabengebiete Relevanz für Liechtenstein haben. Drei dieser Arbeitsgruppen werden nachfolgend detailliert vorgestellt.

7.1.1 Arbeitsgruppen

Im Berichtsjahr beschäftigte sich die *Technology Subgroup* unter anderem mit der Ausarbeitung von Leitlinien zum Thema Blockchain. In diesen werden neben allgemeinen Ausführungen zur Blockchain-Technologie sowohl die verschiedenen Akteure als auch deren Rollen und Verantwortlichkeiten im Hinblick auf die DSGVO beschrieben. Aufgrund der dezentralen Struktur einer Blockchain sowie der verschiedenen Ausprägungsmöglichkeiten einer solchen ist die Qualifizierung eines Verantwortlichen oder eines Auftragsverarbeiters im Sinne der DSGVO nicht immer trivial. Neben weiteren Spannungsfeldern zwischen Blockchain-Technologien und der DSGVO werden in den Leitlinien aber auch Chancen und Möglichkeiten aufgezeigt, wie solche Technologien datenschutzkonform umgesetzt werden können bzw. welche Voraussetzungen dazu erfüllt werden müssen. Einen besonders hohen Stellenwert nehmen dabei die Konzeptphase sowie die anschliessende technische Umsetzung einer Blockchain ein. Art. 25 DSGVO ist entsprechend hoch zu gewichten, da aufgrund der technologischen Eigenschaften einer Blockchain nachträglich konzeptuelle wie auch inhaltliche Anpassungen nur sehr schwer umzusetzen sind. Des Weiteren wird in den Leitlinien auf die Sicherheit der Verarbeitung gemäss Art. 32 DSGVO sowie die DSFA gemäss Art. 35 DSGVO eingegangen. Letztgenannter Artikel nennt insbesondere die Verwendung neuer Technologien als wichtiges Kriterium dafür, dass eine DSFA für eine bestimmte Verarbeitung erforderlich sein kann. Darüber hinaus werden in den Leitlinien auch Möglichkeiten aufgezeigt, wie die Rechte der Betroffenen gewahrt werden können und welche besonderen Aspekte dabei zu beachten sind. Unter gewissen Umständen kann eine Blockchain sogar dazu beitragen, Aspekte der DSGVO einfacher und effizienter umzusetzen. Schliesslich soll in einem eigenen Kapitel speziell auf Kryptowährungen eingegangen werden. Die Datenschutzstelle ist bei der Ausarbeitung dieses Dokuments massgeblich involviert. Aufgrund des komplexen Themengebietes und der bisher wenigen Umsetzungen in der Praxis wird die Veröffentlichung jedoch nicht unmittelbar erfolgen.

Die spezielle *Taskforce Fining* befasste sich im Berichtsjahr mit der Berechnung von Bussgeldern und strebt europaweit eine möglichst einheitliche Herangehensweise an. 2019 wurden von verschiedenen Ländern mehrere Vorschläge eingebracht, wie die Berechnung methodisch systematisiert und europaweit harmonisiert werden könnte, und zwar sowohl für Unternehmen als auch für Privatpersonen. Derzeit wird in der Arbeitsgruppe über die diversen Vorschläge diskutiert und an einer europaweiten methodischen Vereinheitlichung gearbeitet.

Die Datenschutzstelle war 2019 auch in der *International Transfer Subgroup* vertreten, in welcher alle Aspekte, Punkte und Fragen diskutiert werden, die den internationalen Datentransfer betreffen. So sind auch die verbindlichen internen Datenschutzvorschriften *(binding corporate rules; BCR)* jeweils ein Thema. Im Berichtsjahr wurde etwa intensiv darüber diskutiert, wie mit bereits bewilligten oder zurzeit bearbeiteten BCR der britischen Datenschutzaufsichtsbehörde nach dem Brexit umzugehen ist. Da der Brexit jedoch mehrmals hinausgeschoben wurde und im Berichtsjahr auch nicht eintraf, wurde schliesslich lediglich festgehalten, dass die britische Datenschutzaufsichtsbehörde keine weiteren BCR-Verfahren als federführende Behörde mehr annehmen solle. Die betroffenen Fälle wurden sodann anderen Mitgliedstaaten, vornehmlich Spanien und Frankreich, zugeteilt. Daneben wurden in den Sitzungen aber auch konkrete BCR besprochen und evaluiert, ob diese den Anforderungen der Arbeitspapiere *(working papers)* genügen. Die Datenschutzstelle hat bei einer der ersten unter der DSGVO erarbeiteten Stellungnahmen des EDSA zu BCR inhaltlich als Berichterstatter mitgewirkt.

Im Frühjahr 2019 wurde zudem ein zweitägiger Workshop der Arbeitsgruppe zu BCR durchgeführt, in dessen Rahmen insbesondere neue Mitarbeiter der verschiedenen Datenschutzbehörden vom grossen Erfahrungsschatz langjähriger Experten profitieren konnten. Ein Ziel des Workshops war es, ein einheitliches Vorgehen im gesamten EWR-Raum zu etablieren. Als Folge davon wurde das BCR-Genehmigungsverfahren etwas angepasst sowie damit begonnen, gemeinsame Standpunkte und Ansichten *(common views)* bezüglich BCR der Datenschutzbehörden zusammen zu tragen. Auch in diesem Bereich hat sich die Datenschutzstelle als Berichterstatter engagiert. Es ist geplant, dass 2020 die Arbeitspapiere zu BCR aktualisiert und allenfalls weitere hilfreiche Dokumente für Unternehmen veröffentlicht werden.

7.1.2 Gegenseitige Amtshilfe

Wie eingangs erwähnt, erfordert die DSGVO nicht nur eine Zusammenarbeit im bzw. mit dem EDSA, sondern auch eine intensive Kommunikation zwischen den einzelnen europäischen Aufsichtsbehörden, indem diese gemäss Art. 57 Abs. 1 Bst. g DSGVO *«mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten»*. Seit Geltung der DSGVO in Liechtenstein am 20. Juli 2018 ist die Datenschutzstelle daher gemäss Art. 61 DSGVO zur gegenseitigen Amtshilfe verpflichtet. Hierbei handelt es sich um eine neue und zusätzliche Aufgabe, die der Datenschutzstelle mit Inkrafttreten der DSGVO erwachsen ist. Die Datenschutzstelle erhielt im Berichtsjahr 23 Anfragen von anderen europäischen Datenschutzaufsichtsbehörden, was im Vergleich zu den im Vorjahr beantworteten sechs Anfragen 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. Nachfolgend sollen zwei Anfragen von Interesse illustrativ vorgestellt werden:

– *Umfang Auskunftsrecht:* Die slowenische Datenschutzaufsichtsbehörde stellte die Frage, ob im Rahmen der Beantwortung eines Auskunftsgesuchs an ein Unternehmen von diesem auch interne Empfänger der Daten (z. B. einzelne Mitarbeiter), welche die Daten verarbeitet hatten, offengelegt werden müssen. Das Auskunftsrecht gemäss Art. 15 DSGVO umfasst aus Sicht der Datenschutzstelle die eigentlichen Daten, die verarbeitet wurden, sowie die im Artikel genannten Metainformationen wie etwa die Zwecke, für die sie verarbeitet wurden, oder die Empfänger. Letztere sind jedoch nur zu nennen, wenn es sich um externe Empfänger im Sinne von Dritten oder Auftragsverarbeitern handelt. Nicht genannt werden müssen hingegen interne Abteilungen oder gar einzelne Mitarbeiter (Name oder Kontaktdaten), welche die Daten verarbeitet haben.
– *Regress gegen Datenschutzbeauftragte durch Verantwortliche:* Die slowakische Datenschutzaufsichtsbehörde gelangte mit der für Verantwortliche wie für betriebliche Datenschutzbeauftragte gleichermassen bedeutsamen Frage an die Datenschutzaufsichtsbehörden der anderen Mitgliedstaaten, ob Verantwortliche Regress gegen die Datenschutzbeauftragten nehmen können, wenn sie wegen Verstoss gegen eine der in Art. 83 DSGVO genannten Tatbestände von der für sie zuständigen Datenschutzaufsichtsbehörde gebüsst werden.

  Gemäss den Bestimmungen der DSGVO ist der Verantwortliche verantwortlich für die Verarbeitung der personenbezogenen Daten. Die DSGVO sieht keine Bestimmungen vor, welche einen Regress gegen den betrieblichen Datenschutzbeauftragten zulassen würden. Ein Regress gegen den Datenschutzbeauftragten ist damit aus Sicht der Datenschutzstelle nur in einem zivilgerichtlichen Verfahren bei grobfahrlässigem Verhalten oder wissentlich herbeigeführtem Datenschutzverstoss durch den Datenschutzbeauftragten möglich.

7.2 Europarat

Die Datenschutzstelle konnte im Berichtsjahr dank der nun verfügbaren personellen Ressourcen wieder an beiden Versammlungen des Beratenden Ausschusses des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) des Europarats in Strassburg teilnehmen. Dieses Übereinkommen wurde kürzlich mittels eines Änderungsprotokolls modernisiert und insbesondere an die heutigen informations- und kommunikationstechnologischen Möglichkeiten der Datenverarbeitung angepasst. Die Datenschutzstelle war 2019 massgeblich beteiligt an der deutschen Übersetzung dieses Protokolls und wird im laufenden Jahr den Ratifikationsprozess in Liechtenstein begleiten.

Nach den im Januar verabschiedeten Leitlinien zum Thema künstliche Intelligenz und Datenschutz bestand die Hauptarbeit des Beratenden Ausschusses im Berichtsjahr in der Erarbeitung von Berichten und Positionspapieren zu den Themen Gesichtserkennung, Datenschutz im Bildungswesen, Profiling und grenzüberschreitender Zugang zu Daten in der Strafverfolgung. Die Ergebnisse können zu künftigen Handlungsempfehlungen, Resolutionen oder Erklärungen übergeordneter Organe des Europarates führen.

«Eine Hauptaufgabe der Datenschutzstelle wird 2020 sein, einen Datenschutz der zwei Geschwindigkeiten in Liechtenstein zu verhindern und auch jene Institutionen zu erreichen, die den Datenschutz noch nicht auf ihrer To-Do-Liste stehen haben.»

8. Schlussbemerkung und Ausblick

Wie eingangs angekündigt, sollte dieser Tätigkeitsbericht eine erste Zwischenbilanz ziehen zur Umsetzung der seit Sommer 2018 in Liechtenstein geltenden DSGVO und des am 1. Januar 2019 in Kraft getretenen DSG. Insgesamt fällt diese Bilanz aus Sicht der Datenschutzstelle durchwegs positiv aus. Trotz grosser Herausforderungen konnte im Berichtsjahr vieles erreicht werden.

Die Hauptaufgabe im Jahr 2020 wird weiterhin die Klärung der vielen offenen Fragen rund um die Auslegung der DSGVO bleiben, denn nach wie vor findet sich eine Fülle von Streitfragen, die bislang zwar in Literatur und Praxis für Diskussionsstoff sorgten, für die es aber noch keine klaren und verbindlichen Vorgaben gibt. Nicht wenige dieser Fragen betreffen die EWR-weite Zusammenarbeit zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss. Ein weiteres Problemfeld eröffnet sich beim Zusammenspiel von Anforderungen unter der DSGVO und deren praktischer Umsetzung mit Hilfe der einzelnen nationalen Verfahrensvorschriften. Aber auch auf nationaler Ebene, bei den Verantwortlichen und Auftragsverarbeitern, sind noch zahlreiche Fragen offen bzw. kommen angesichts der stetigen technischen Weiterentwicklung neue hinzu.

2020 wird der Beratung und Informationsvermittlung in der Datenschutzstelle abermals oberste Priorität eingeräumt. Der Informationsfluss soll gewährleisten, dass öffentliche und private Stellen ihre Prozesse rechtssicher planen können. Die in den vergangenen beiden Jahren erfolgreich eingesetzten Kommunikationskanäle sollen weiter genutzt und verbessert sowie Anregungen von Seiten der datenverarbeitenden Stellen oder der Bevölkerung soweit als möglich umgesetzt werden. Als neues Instrument der Informationsvermittlung wird die Datenschutzstelle 2020 zwei Workshops zu den beiden aktuellen Themen Videoüberwachung und Beschäftigtendatenschutz anbieten. Im Rahmen dieser Veranstaltungen sollen die Teilnehmenden unter der Leitung von Moderatoren unterschiedliche Praxisfälle lösen und somit auf die praktische Umsetzung der Datenschutzanforderungen in diesen beiden Spezialbereichen bestens vorbereitet werden.

In Bezug auf die Beratung und Sensibilisierung soll 2020 eine Bevölkerungsgruppe besondere Beachtung finden, die bislang noch nicht im Fokus der Tätigkeit der Datenschutzstelle stand. Die Senioren und ihre speziellen Bedürfnisse in der digitalen Welt sollen ein Schwerpunkt der Beratungstätigkeit 2020 werden. Aber auch Kinder und Jugendliche werden 2020 erneut nicht zu kurz kommen.

Nicht fehlen darf beim Ausblick natürlich auch die Aufsicht. Die Bearbeitung von Beschwerden betroffener Personen, aber auch amtswegige Datenschutzüberprüfungen werden auf der nächstjährigen Agenda der Datenschutzstelle stehen. Gerade letztere haben im Berichtsjahr aufgezeigt, dass sie absolut notwendig sind, um einen Datenschutz der zwei Geschwindigkeiten in Liechtenstein zu verhindern und auch jene Institutionen zu erreichen, die den Datenschutz noch nicht auf ihrer To-Do-Liste stehen haben.

Datenschutzstelle Fürstentum Liechtenstein
Städtle 38
Postfach 684
FL-9490 Vaduz

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