dsb

Republik Österreich

Datenschutz behörde

Datenschutzbericht 2016

Datenschutzbericht 2016

Wien, im März 2017

Impressum

Medieninhaber, Herausgeber und Redaktion:
Datenschutzbehörde, Dr. Andrea Jelinek
(gemäß § 35ff DSG 2000), Hohenstaufengasse 3, 1010 Wien
Kontakt: dsb@dsb.gv.at
Website: www.dsb.gv.at
Fotonachweis: Pollmann (Seite 5)
Gestaltung: Datenschutzbehörde
Druck: BM.I Digitalprintcenter
Wien, 2017

Inhalt

1 Vorwort

Die unabhängige Datenschutzbehörde (DSB) ist seit 1. Jänner 2014 die nationale Kontrollstelle im Sinne des Art. 28 der Datenschutzrichtlinie 95/46/EG. Zu ihren Aufgaben zählt die Führung von Individualverfahren auf Antrag, aber auch des Datenverarbeitungs- und des Stammzahlenregisters. Zudem führt die DSB amtswegige datenschutzrechtliche Überprüfungen durch und ist als aktives Mitglied in zahlreichen internationalen und nationalen Gremien präsent.

Da in den Jahren 2014 und 2015 die Struktur der Behörde geändert und in der Folge gefestigt wurde, konnte im Jahr 2016 begonnen werden, die Mitarbeiterinnen und Mitarbeiter der Behörde auf die Geltung der Datenschutzgrundverordnung ab 25. Mai 2018 vorzubereiten. Mannigfache Maßnahmen wurden bereits getroffen und werden im Jahr 2017 forciert und erweitert werden. Die Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörde waren bereits im Jahr 2016, und werden noch mehr im Jahr 2017 als Vortragende für die Datenschutzgrundverordnung angefragt. Wenn es die Zeit irgendwie zulässt, kommen wir diesen Einladungen auch sehr gerne nach, zumal es mich als Leiterin der Behörde besonders freut, dass die Awareness für den Datenschutz in den letzten Jahren merklich gestiegen ist. Die Herausforderungen der Datenschutzgrundverordnung treffen die Datenschutzbehörde, die öffentlichen Einrichtungen und die Unternehmen im gleichen Maß, lediglich die Intensität und die Seite des Zaunes sind unterschiedlich.

Der Datenschutzbericht 2016 ist der dritte, gemäß § 37 Abs. 5 DSG 2000, jährlich zu erstellende Bericht über die Tätigkeit der Datenschutzbehörde, der dem Bundeskanzler bis 31. März des Folgejahres zu übergeben und in geeigneter Weise durch die Behörde zu veröffentlichen ist. Die Veröffentlichung wird auf der Homepage der Datenschutzbehörde erfolgen.

Interessierte können sich auch während des Jahres über die Tätigkeiten der Datenschutzbehörde informieren; der seit 01/2015 quartalsmäßig erscheinende Newsletter der DSB gibt einen guten Überblick über Neuerungen, Judikatur und sonstige interessante Bereiche aus der nationalen und internationalen Welt des Datenschutzes.

Dr. Andrea Jelinek
Leiterin der Datenschutzbehörde

2 Die Datenschutzbehörde

2.1 Organisation und Aufgaben

2.1.1 Organisation

Die Datenschutzbehörde ist monokratisch strukturiert, aufgrund europarechtlicher und völkerrechtlicher Vorgaben unabhängig und keiner Dienst- und Fachaufsicht unterworfen.

Die Leiterin der Datenschutzbehörde ist Dr. Andrea Jelinek, der stellvertretende Leiter Dr. Matthias Schmidl. Beide wurden vom Bundespräsidenten auf Vorschlag der Bundesregierung mit 1. Jänner 2014 für die Dauer von fünf Jahren bestellt. Wiederbestellungen sind zulässig.

2.1.2 Aufgaben

Die Datenschutzbehörde ist insbesondere zuständig für die Behandlung von Eingaben von Personen, die sich durch Tätigkeiten eines Dritten (z.B. Unternehmer, Nachbar, Behörde etc.) in datenschutzrechtlichen Rechten (Geheimhaltung, Auskunft, Richtigstellung, Löschung) verletzt erachten.

Im Rahmen eines antragsbedürftigen Beschwerdeverfahrens nach § 31 DSG 2000 kann die Datenschutzbehörde eine Rechtsverletzung mit Bescheid feststellen.

Das Kontroll- und Ombudsmannverfahren nach § 30 DSG 2000 ist ein Verfahren, das auf die Herstellung des rechtmäßigen Zustandes abzielt und entweder auf Antrag oder von Amts wegen geführt wird. Dieses Verfahren ist im Bereich des soft law angesiedelt und hat mediativen Charakter. Die Datenschutzbehörde kann gegebenenfalls Empfehlungen aussprechen und veröffentlichen. Bescheide können in diesem Verfahren, abgesehen von Mandatsbescheiden nach § 30 Abs. 6a DSG 2000, nicht erlassen werden.

Die Datenschutzbehörde hat die Verwendung von Daten für wissenschaftliche Forschung und Statistik oder die Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen (§§ 46 und 47 DSG 2000) in bestimmten Fällen mit Bescheid zu genehmigen.

Darüber hinaus genehmigt die Datenschutzbehörde, in bestimmten Fällen den Transfer von Daten in Drittländer mit Bescheid (§ 13 DSG 2000).

Die zahlenmäßig umfangreichste Aufgabe der Datenschutzbehörde besteht in der Erteilung von Rechtsauskünften an Bürgerinnen und Bürger. Die Datenschutzbehörde kann jedoch nur insoweit Rechtsauskünfte erteilen, als damit nicht eine allfällige Entscheidung in einem konkreten Beschwerde-, Kontroll- oder Registrierungsverfahren vorweggenommen wird. Im Regelfall wird daher abstrakt und nicht fallbezogen eine Rechtsauskunft erteilt.

Darüber hinaus führt die Datenschutzbehörde das Datenverarbeitungsregister. Grundsätzlich ist eine Datenanwendung vor Inbetriebnahme vom jeweiligen Auftraggeber dem Datenverarbeitungsregister zu melden (§§ 17 ff DSG 2000). Lehnt die Datenschutzbehörde die Registrierung der Datenanwendung nicht ab, ist sie in der Folge im online-basierten Datenverarbeitungsregister für jedermann kostenlos einsehbar. Wird die Registrierung abgelehnt, so kann der Auftraggeber beantragen, dass die Behörde mit Bescheid darüber abspricht. Die Datenschutzgrundverordnung kennt kein Register mehr (beachte jedoch: Datenschutzfolgeabschätzung in der Verantwortung des jeweiligen datenschutzrechtlich Verantwortlichen).

Alle Bescheide der Datenschutzbehörde können mit Beschwerde an das Bundesverwaltungsgericht bekämpft werden. Dieses entscheidet im Dreiersenat (ein Berufsrichter, zwei Laienrich-

ter, § 39 DSG 2000). Entscheidungen des Bundesverwaltungsgerichtes können – auch von der Datenschutzbehörde – mit Revision an den Verwaltungsgerichtshof bzw. Beschwerde an den Verfassungsgerichtshof bekämpft werden.

Das E-Government-Gesetz überträgt der Datenschutzbehörde die Funktion der Stammzahlenregisterbehörde. In diesem Kontext obliegen der Datenschutzbehörde auch die Führung des Ergänzungsregisters sowie die Errechnung von Stammzahlen.

Darüber hinaus ist die Datenschutzbehörde in internationalen Foren auf EU-Ebene sowie des Europarates vertreten und arbeitet mit ihren Partnerbehörden eng zusammen.

Die Datenschutzbehörde stellt auf der Webseite der DSB (https://www.dsb.gv.at/rechte-der-betroffenen) allgemeine Informationen zu den Verfahren vor der Datenschutzbehörde sowie Musterformulare für Eingaben zur Verfügung.

Informationen zum Meldeverfahren werden auf der Webseite der DSB (https://www.dsb.gv.at/zugang-zu-dvr-online) bereitgestellt.

Die Entscheidungen der Datenschutzbehörde werden nur dann im RIS veröffentlicht, wenn sie von der Rechtsprechung der ehemaligen Datenschutzkommission abweichen, es keine Rechtsprechung der Datenschutzkommission zu einer Rechtsfrage gibt oder diese Rechtsprechung uneinheitlich ist. Die Veröffentlichung erfolgt grundsätzlich dann, wenn keine Anfechtung vor dem Bundesverwaltungsgericht erfolgt.

2.2 Der Personalstand

Im Berichtszeitraum versahen 26 Personen in Teil- oder Vollzeit ihren Dienst bei der Datenschutzbehörde, davon 13 Juristinnen und Juristen, 4 Mitarbeiterinnen im gehobenen Dienst und 9 Mitarbeiterinnen und Mitarbeiter im Fachdienst (zwei davon in Karenz und 1 MA einer anderen Dienststelle des Bundes dienstzugeteilt). Die Bediensteten der Datenschutzbehörde sind in Erfüllung ihrer Aufgaben an die Weisungen der Leitung gebunden.

Die Vorbereitungen auf die Datenschutzgrundverordnung (siehe auch die Ausführungen zu Punkt 5 des Berichts) zeigen deutlich, dass die Datenschutzbehörde mit 2018 jedenfalls – wie alle anderen Datenschutzbehörden in Europa auch – zusätzlichen Personalbedarf haben wird, der auch bereits angemeldet wurde und verhandelt wird.

Der Behörde wachsen neue Aufgaben zu, deren Erfüllung nicht durch den Wegfall des Datenverarbeitungsregisters (und der Arbeit in diesem Bereich) kompensiert werden kann. Da zum Zeitpunkt des Redaktionsschlusses dieses Berichts noch kein Entwurf eines nationalen Datenschutzgesetzes vorliegt, kann der genaue Personalbedarf an dieser Stelle nicht angegeben werden.

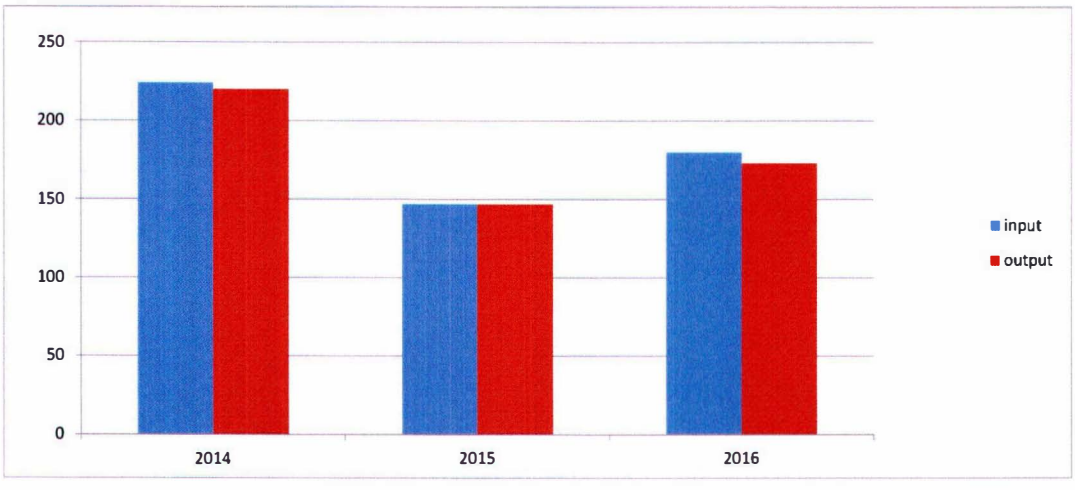
3 Tätigkeit der Datenschutzbehörde

3.1 Statistische Darstellung

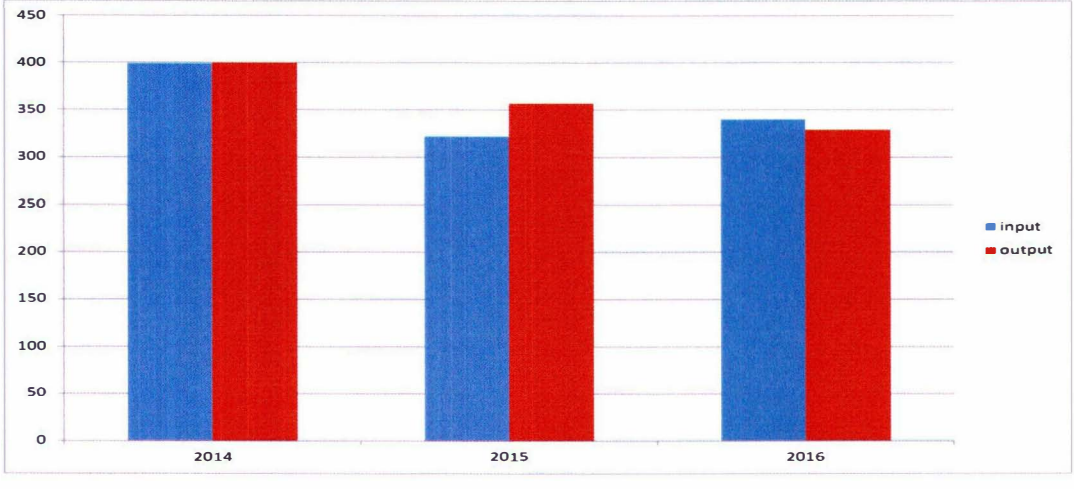
Tabelle 1 Anzahl der Eingangsstücke und Erledigungen

	Eingangsstücke			Erledigungen		
Art der Tätigkeit	**2014**	**2015**	**2016**	**2014**	**2015**	**2016**
Individualbeschwerden	224	147	180	220	147	173
Erledigungsart der Individualbeschwerden	224	147	173	117 Bescheide 103 Einstellungen	95 Bescheide 52 Einstellungen	122 Bescheide 51 Einstellungen
Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (Verfahren über Antrag)	399	332	340	400	357	329
Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (amtswegiges Prüfverfahren)	98	67	90	88	97	80
Rechtsauskünfte	2261	2152	2004	2261	2123	1980
Genehmigungen nach § 46 und 47 DSG 2000 (wissenschaftliche Forschung u Statistik)	11	16	23	14	18	18
Genehmigungen im Internationalen Datenverkehr	79	128	312	80	150	254
Auskunft Schengen	33	10	20	33	7	20
Verfahren vor dem Bundesverwaltungsgericht		31	34			

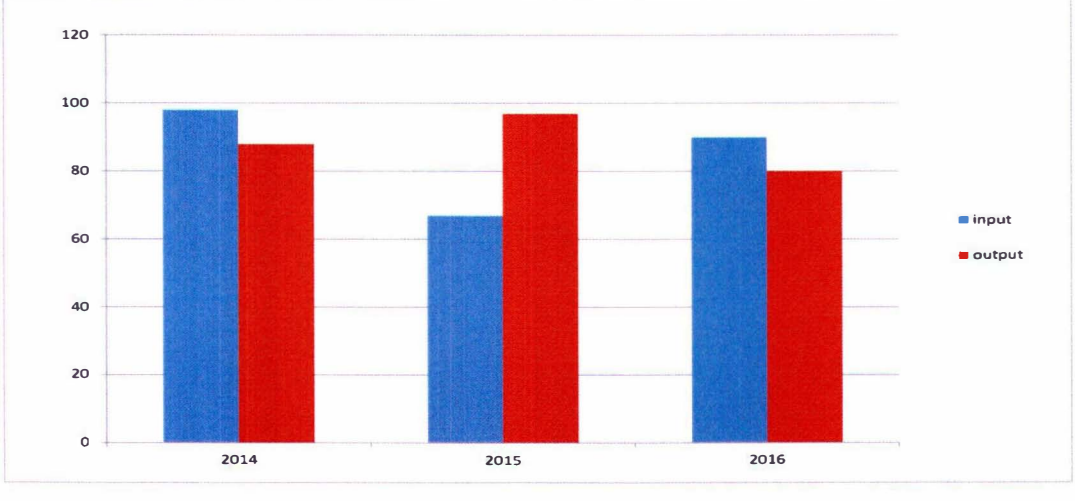
Individualbeschwerden § 31 DSG 2000



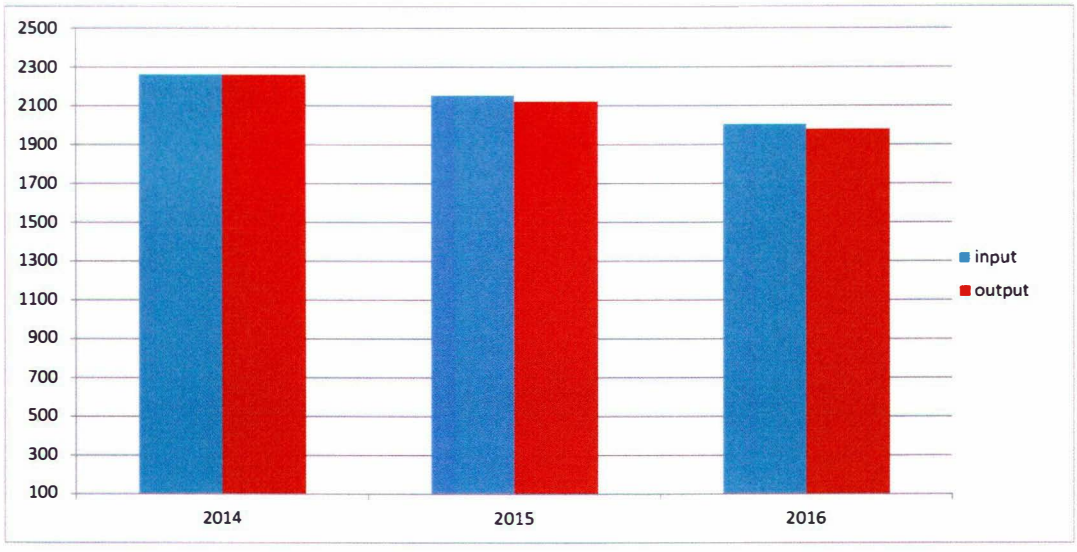
Kontroll- und Ombudsmannverfahren (§ 30 DSG 2000)



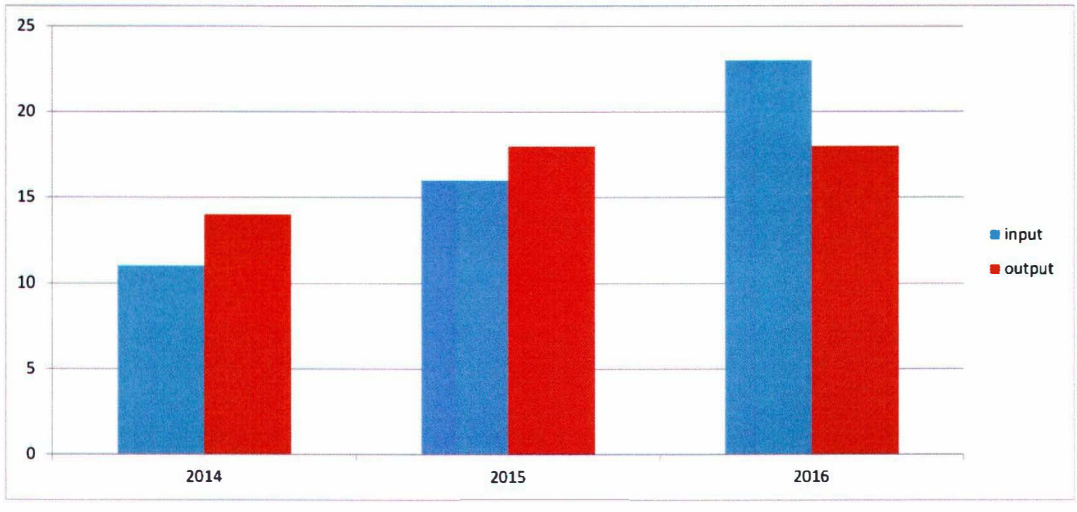
amtswegiges Prüfverfahren (§ 30 Abs. 2 DSG 2000)



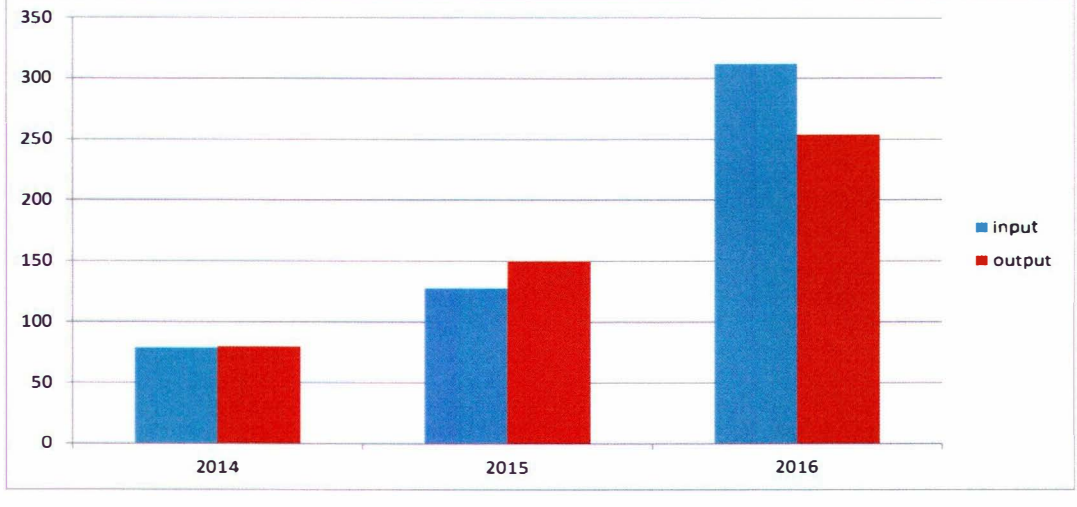
Rechtsauskünfte



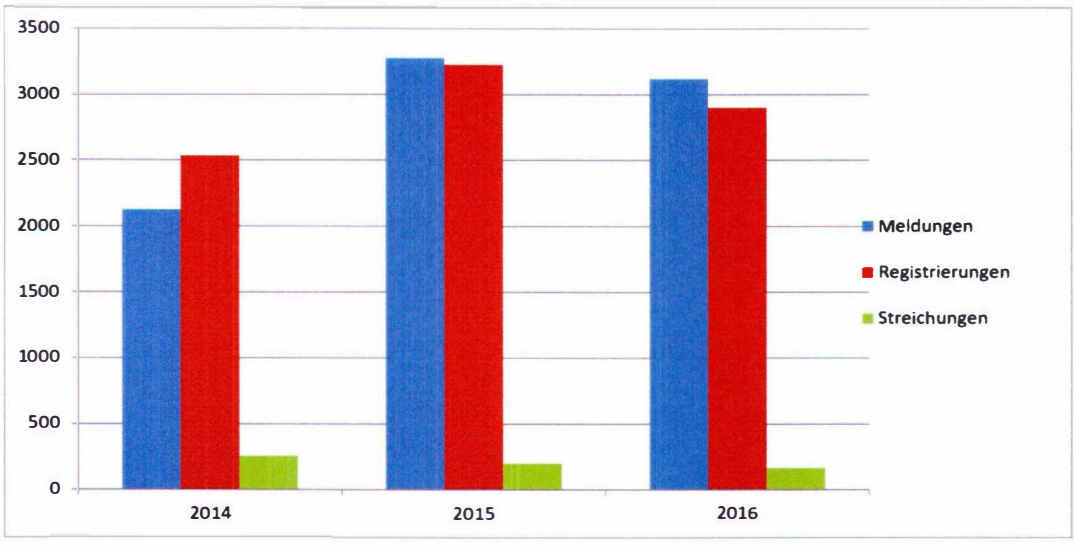
Genehmigung nach § 46 und 47 DSG 2000



Genehmigung im Internationalen Datenverkehr (§§ 12 und 13 DSG 2000)



Auftraggeber



Datenanwendungen

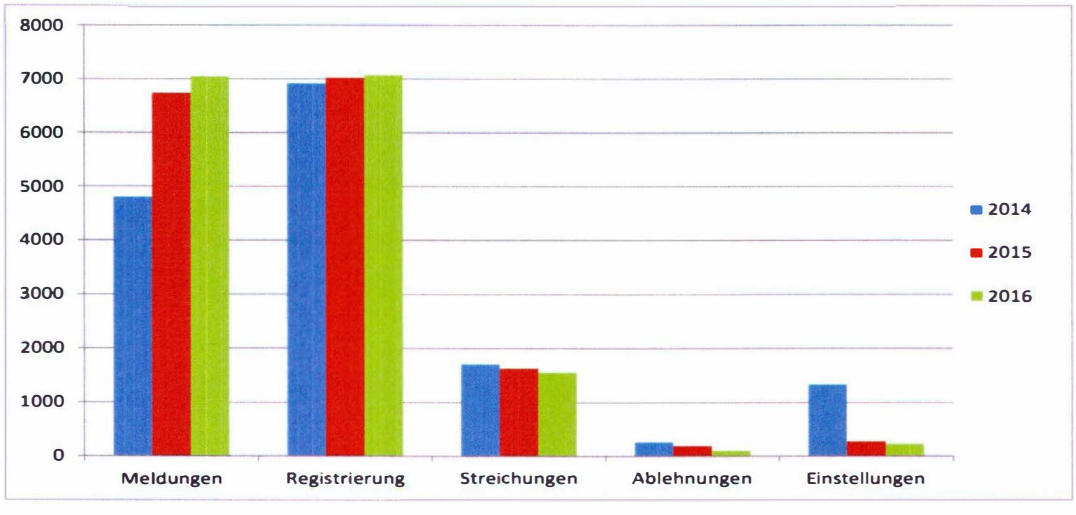


Tabelle 2 Anzahl der Tätigkeiten des Datenverarbeitungsregisters

Tätigkeiten	2014	2015	2016
Tätigkeiten für Auftraggeber in Summe	**4918**	**6703**	**6186**
Meldungen	2125	3276	3119
Registrierungen	2533	3226	2901
davon automatisch registriert	*1188 (ca. 47 %)*	*2365 (ca. 73 %)*	*2135 (ca. 73 %)*
davon durch das DVR registriert	*1345 (ca. 53 %)*	*861 (ca. 27 %)*	*766 (ca. 27 %)*
Streichungen	260	201	166
Tätigkeiten in Datenanwendungen in Summe	**15039**	**15872**	**16007**
Meldungen	4802	6741	7045
davon automatisch registriert	*2340 (ca. 48 %)*	*3985 (ca. 59 %)*	*4300 (ca. 61 %)*
davon vom DVR überprüft	*2462 (ca. 52 %)*	*2756 (ca. 41 %)*	*2745 (ca. 39 %)*
Registrierungen	6917	7028	7072
Streichungen	1712	1633	1558
Ablehnungen	263	191	105
Einstellungen	1331	279	227
Verbesserungsaufträge in Summe	**1175**	**1073**	**1009**
Bescheide im Registrierungsverfahren	8	8	3
Verfahren gemäß § 22a DSG 2000	6	9	2
Rechtsunwirksam eingebrachte Meldungen	123	112	104
Meldungen von Rechtsnachfolgen	58	44	57

3.2 Verfahren und Auskünfte

3.2.1 Individualbeschwerden

Allgemeines und Grundsätzliches

Das Beschwerdeverfahren nach § 31 DSG 2000 ist das wichtigste Rechtsschutzverfahren im Zuständigkeitsbereich der Datenschutzbehörde.

Beschwerden wegen Verletzung der Rechte auf Auskunft, Geheimhaltung, Löschung oder Richtigstellung (§ 31 Abs. 2 DSG 2000) sind gegen alle datenschutzrechtlichen Auftraggeber der öffentlichen Verwaltung möglich; gegen Auftraggeber aus dem privaten Bereich sind nur Beschwerden wegen Verletzung des Rechts auf Auskunft (§ 31 Abs. 1 DSG 2000) zulässig. Akte der Gesetzgebung und Gerichtsbarkeit sind von der Zuständigkeit der Datenschutzbehörde ausgenommen.

Der inhaltliche Schwerpunkt im österreichischen datenschutzrechtlichen Beschwerdeverfahren liegt somit bei Themen aus dem Bereich der innerstaatlichen öffentlichen Verwaltung und bei der Auskunftserteilung durch private Rechtsträger.

Formell handelt es sich um ein Verwaltungsverfahren nach dem Allgemeinen Verwaltungsverfahrensgesetz 1991 (AVG). Die Beschwerde gemäß § 31 DSG 2000 ist ein förmlicher Rechtsschutzantrag an die Datenschutzbehörde.

Inhaltlich handelt es sich meist um ein Zweiparteienverfahren, in dem die Seiten gegensätzliche Standpunkte vertreten (= kontradiktorisches Verfahren). Die Parteien werden als Beschwerdeführer und Beschwerdegegner bezeichnet.

Der Datenschutzbehörde kommt von Gesetzes wegen die Rolle einer unabhängigen Streitentscheidungsinstanz zu (§ 31 Abs. 1, 2 und 7, § 37 Abs. 1 DSG 2000). Die Entscheidungen im Verfahren werden durch die Leiterin der Datenschutzbehörde oder in ihrem Namen durch einen aufgrund einer Ermächtigung handelnden Vertreter getroffen. Die ermächtigten Vertreter sind an allfällige Weisungen der Leiterin gebunden.

Im Verfahren wegen Verletzung der Rechte auf Auskunft, Löschung oder Richtigstellung muss dem Beschwerdeverfahren vor der Datenschutzbehörde zwingend ein „Vorverfahren" zwischen Betroffenem und Auftraggeber vorangegangen sein, in dem ersterer das jeweilige Recht geltend gemacht hat. Dieser Schriftwechsel muss der Datenschutzbehörde vorgelegt werden (§ 31 Abs. 4 DSG 2000). Ein Fehlen des entsprechenden Nachweises wird als Inhaltsmangel behandelt, der bei Nichtbehebung zur Zurückweisung der Beschwerde (mit Bescheid) führt.

Werden die Rechte auf Auskunft, Löschung oder Richtigstellung vom Betroffenen gegenüber einer Verwaltungsbehörde oder einem anderen datenschutzrechtlich Verantwortlichen (Auftraggeber) des öffentlichen Bereichs geltend gemacht, so ist auch eine Behörde, unabhängig von der Bezeichnung des Anbringens („Antrag auf Richtigstellung von Daten") nicht verpflichtet, die Sache durch einen Bescheid zu erledigen. In jedem Fall muss aber eine Mitteilung ergehen. Diese, bis auf die Schriftlichkeit nicht formgebundene, Mitteilung des Auftraggebers ist im Anschluss gegebenenfalls im Beschwerdeverfahren von der Datenschutzbehörde zu überprüfen. Die verwaltungsgerichtliche Kontrolle beginnt erst nach einem Zwischenschritt in Form eines Bescheids der Datenschutzbehörde. Dieses Abweichen von dem in Art. 130 Abs. 2 Z 1 des Bundes-Verfassungsgesetzes angelegten System ist durch Unionsrecht bedingt (Art. 28 der Richt-

linie 95/46/EG; Garantie des Bestehens einer unabhängigen Kontrollstelle für Datenschutz in Art. 8 Abs. 2 der Charta der Grundrechte der EU)

Praxis der Beschwerdeverfahren im Jahr 2016

Erfahrungsgemäß machen sich in den Medien präsente Themen oder bekannt gewordene Missstände schnell dahingehend bemerkbar, dass die Zahl der Beschwerden aus einem bestimmten Themenkreis oder gegen einen bestimmten Auftraggeber plötzlich steigt, um in den Folgejahren ebenso schnell wieder zu fallen. Im Berichtsjahr lag, erkennbar an Hand der dokumentierten Entscheidungen, ein deutlicher Schwerpunkt der Beschwerdeverfahren bei der Durchsetzung des Auskunftsrechts.

Aus den Beobachtungen der DSB ergibt sich weiters die nicht durch statistische Daten belegbare Vermutung, dass der typische im Beschwerdeverfahren Rechtsschutz suchende Bürger nicht zur Gruppe der „Netizens" (in Online-Netzwerken präsente und vernetzte Menschen) gehört. Diskussionen in bekannten sozialen Netzwerken wie Facebook und Twitter scheinen weiterhin selten oder nie den Anstoß für ein gehäuftes Auftreten von typisierbaren Beschwerden (gleicher Inhalt, gleiche Adressaten) zu geben.

Im Jahr 2016 waren Fälle zu beobachten, in denen insbesondere das Recht auf Auskunft und die daran anknüpfenden Rechtschutzverfahren erkennbar dazu verwendet worden sind, aus abseits der Sorge um das Grundrecht auf Datenschutz liegenden Motiven verschiedene Auftraggeber in Verfahren und Rechtsstreitigkeiten zu verwickeln. Da das Recht auf Auskunft als objektives Kontrollrecht ohne Offenlegung eines Grundes ausgeübt werden kann, ist ein solches Vorgehen rechtmäßig, solange es nicht ausschließlich in der Absicht erfolgt, dem Auftraggeber Nachteile zuzufügen (= Schikane). Nachgewiesene Fälle von Schikane im Beschwerdeverfahren liegen der Datenschutzbehörde bis heute nicht vor, es wurde dies aber von unterlegenen Auftraggebern mehrfach in Beschwerdesachen vor dem Bundesverwaltungsgericht behauptet und gegen das Bestehen eines Rechts auf Auskunft eingewendet. Das Bundesverwaltungsgericht hat sich zu dieser Frage noch nicht geäußert.

Die durch die DSG-Novelle 2010 eingeführte Möglichkeit, Beschwerdeverfahren als „gegenstandslos" durch Einstellung zu beenden (§ 31 Abs. 8 DSG 2000), ist auch im Jahr 2016 eine wesentliche Vereinfachung der Arbeit der Datenschutzbehörde. Sie ermöglicht es insbesondere, Beschwerdeverfahren wegen Auskunfts- oder Löschungsverlangen, auf die der Auftraggeber in gesetzwidriger Weise zunächst nicht reagiert hat, nach Erreichung des primären Verfahrensziels (Beantwortung des Auskunfts- oder Löschungsverlangens) ohne großen Aufwand zu beenden. Im Jahr 2016 wurden 51 Beschwerdeverfahren durch Einstellung (Beschwerdezurückziehungen aus anderen Gründen eingeschlossen) beendet. Die Praxis dieser Form der Verfahrensbeendigung wegen Klaglosstellung wurde mehrfach durch das Bundesverwaltungsgericht als rechtmäßig bestätigt.

Ausgewählte Beschwerdeentscheidungen aus 2016

Die Datenschutzbehörde hat in ihrer öffentlich zugänglichen Entscheidungsdokumentation (im Rahmen des Rechtsinformationssystems des Bundes – RIS; Stand: 9. Februar 2017) aus dem Jahr 2016 sechs Bescheide aus Beschwerdeverfahren dokumentiert. Diese Zahl kann sich (z.B. wegen Rechtsmittelentscheidungen des BVwG, VfGH oder VwGH) selbst nach Erscheinen des Datenschutzberichts 2016 ändern.

Durch die Etablierung des Bundesverwaltungsgerichts als Rechtsmittelinstanz wurde die Bedeutung der Rechtsprechung der Datenschutzbehörde für die verbindliche Auslegung und Weiterentwicklung des Datenschutzrechts redimensioniert. Regelmäßig werden daher nur

rechtskräftige Entscheidungen dokumentiert, Ausnahmefälle sind in den RIS-Dokumenten durch entsprechende Vermerke gekennzeichnet. In diesen Fällen wird die Entscheidung nach einer Aufhebung aus dem RIS entfernt oder der sonstige Ausgang des Verfahrens dokumentiert

Die wichtigsten Beschwerdeentscheidungen in chronologischer Reihenfolge:

a. Bescheid vom 8.2.2016, DSB-D122.304/0012-DSB/2015 (Auskunftsrecht gegenüber einem Wirtschaftsauskunftsdienst, logischer Ablauf der automatisierten Entscheidungsfindung, nicht rechtskräftig)

Der Beschwerdeführer hatte sein Recht auf Auskunft gegenüber einer Ges.m.b.H. (Beschwerdegegnerin) ausgeübt, die einen Wirtschaftsauskunftsdienst betreibt und seine Bonität (Kreditwürdigkeit) beurteilt hatte. Neben einer allgemeinen Auskunft über seine Daten hatte er auch Auskunft über automatisierte Einzelentscheidungen gemäß § 49 DSG 2000 verlangt. Die Auskunft über den logischen Ablauf der automatisierten Entscheidungsfindung (§ 49 Abs. 3 DSG 2000) wurde ihm verweigert. Die Beschwerdegegnerin brachte nach Einbringung einer Beschwerde bei der Datenschutzbehörde dazu vor, eine Auskunft über den logischen Ablauf der automatisierten Bonitätsbeurteilung würde Geschäftsgeheimnisse und Urheberrechte verletzen. Außerdem treffe die Beschwerdegegnerin keine Entscheidung sondern liefere ihren Kunden nur Informationen für eine geschäftliche Entscheidung, sei daher nur Dienstleister von Dritten. Die Datenschutzbehörde folgte in ihrem Bescheid diesen Argumenten nicht und hielt fest, dass Wirtschaftsauskunftsdienste Betroffenen in allgemein verständlicher Form über den logischen Ablauf der Entscheidungsfindung einer automatisierten Bonitätsprüfung (Überprüfung der Kreditwürdigkeit) Auskunft erteilen müssen. Sie können sich dabei nicht generell auf eine Dienstleisterrolle zurückziehen und den Betroffenen an ihre Kunden (als „Auftraggeber" der Bonitätsprüfung) verweisen. Eine generelle Auskunftsverweigerung über die Entscheidungslogik unter Berufung auf ein Geschäftsgeheimnis oder Urheberrechte an entsprechenden Computerprogrammen ist nicht zulässig. Entscheidend ist, dass der Wirtschaftsauskunftsdienst seinen Kunden durch eine automatisierte Bewertung im Einzelfall Entscheidungsgrundlagen für einen Geschäftsabschluss oder eine Kreditgewährung liefert. Der Wirtschaftsauskunftsdienst muss die daraus folgende Entscheidung aber nicht selbst treffen, um der Auskunftspflicht nach § 49 Abs. 3 DSG 2000 zu unterliegen. Der Beschwerde wurde daher teilweise Folge gegeben. Gegen diesen Bescheid hat die Beschwerdegegnerin Beschwerde an das Bundesverwaltungsgericht erhoben (anhängig zu Zl. W101 2124657-1).

b. Bescheid vom 10.3.2016, DSB-D122.322/0001-DSB/2016 (Auskunftsrecht gegenüber einem Direktmarketingunternehmen, Zuschreibung von Marketingklassifikationen)

Der Beschwerdeführer hatte sein Recht auf Auskunft gegenüber einer das Gewerbe des Direktmarketingunternehmens ausübenden Ges.m.b.H. (Beschwerdegegnerin) geltend gemacht. Neben einer allgemeinen Auskunft über seine Daten hatte er auch Auskunft über automatisierte Einzelentscheidungen gemäß § 49 DSG 2000 verlangt. Nach Erhalt einer Auskunft (bzw. einer ergänzenden Auskunft während des bereits anhängigen Beschwerdeverfahrens) machte der Beschwerdeführer insbesondere geltend, dass ihm gemäß § 49 Abs. 3 DSG das Recht zukomme, den logischen Ablauf der automatisierten Entscheidungsfindung bei Marketingklassifikationen dargelegt zu erhalten, was ihm verweigert worden sei. Die Datenschutzbehörde stellte (nach einer Einschau in die Datenanwendungen der Beschwerdegegnerin im Ermittlungsverfahren) u.a. fest, dass die Beschwerdegegnerin zur Klassifizierung der Daten für Marketingzwecke ein auf soziodemografischen Erkenntnissen beruhendes System verwendet, nach dessen Anwendung der Beschwerdeführer der Gruppe der „digitalen Individualisten" zugerechnet wurde. Dies wurde dem Beschwerdeführer im Zuge der Auskunftserteilung auch offengelegt. Die

Zuschreibung von Marketingklassifikationen, die der Beschwerdegegnerin gemäß § 151 Abs. 6 GewO 1994 erlaubt war, ist nach Ansicht der Datenschutzbehörde jedoch, anders als eine Bonitätsprüfung (siehe Entscheidung a. oben), kein Vorgang der automatisierten Einzelentscheidung, der dem besonderen Auskunftsrecht gemäß § 49 Abs. 3 DSG 2000 (bzw. Art. 15 Abs. 1 RL 95/46/EG) unterliegt. Die Beschwerde wurde daher abgewiesen. Dieser Bescheid ist rechtskräftig.

c. Bescheid vom 15.4.2016, DSB-D122.418/0002-DSB/2016 (Auskunftsrecht gegenüber einem Mobilfunkunternehmen, Standortdaten, Cell-ID)

Die Beschwerdeführerin verlangte von einer ein Mobilfunknetz betreibenden Kapitalgesellschaft (Beschwerdegegnerin) Auskunft über die gespeicherten Standortdaten von zwei ihr zuzuordnenden Mobilfunkanschlüssen in einem bestimmten Zeitraum. Dazu verwies sie auf die Pflicht der Beschwerdegegnerin gemäß § 90 Abs. 8 TKG 2003. Die Beschwerdegegnerin verweigerte diese Auskunft mit der Begründung, eine Verwendung solcher Verkehrsdaten sei nur in bescheinigten Notfällen für Notfalldienste oder in polizeilichen Ermittlungsverfahren bzw. auf richterliche Anordnung hin zulässig. Die Datenschutzbehörde hielt in ihrem Bescheid fest, dass keine Feststellung erfolgen konnte, dass die Beschwerdeführerin im Zeitraum, für den Auskunft verlangt wurde, stets die „tatsächliche Nutzerin" der den Anschlüssen zuzurechnenden Geräte war. In Großstädten sind die Funkzellen von Mobilfunknetzen klein (300 bis 500 m Durchmesser und ermöglichen allein durch das Einbuchen der mobilen Telekommunikationsendeinrichtung in die nächstgelegene Funkzelle auf Grund der verarbeiteten Cell-ID eine Standortbestimmung des jeweiligen Nutzers des Mobiltelefons. Der Teilnehmer (Vertragsinhaber) kann auf Grund häufiger Ausnahmen (z.B. Kinder, Unternehmensanschlüsse) nicht mit dem tatsächlichen Nutzer gleichgesetzt werden. Das Fernmelderecht räumt gemäß §§ 92 Abs. 1 iVm 100 Abs. 1 TKG 2003 dem Betroffenen nur ein auf den Erhalt eines Einzelentgeltnachweises eingeschränktes Recht ein, über gespeicherte Verkehrsdaten Auskunft zu erhalten. Auch diese Beschränkung geht als Spezialvorschrift dem allgemeinen Auskunftsrecht gemäß § 26 DSG 2000 vor. Da die Beschwerdegegnerin die Auskunft begründet abgelehnt hatte, wurde die Beschwerde abgewiesen. Der Bescheid ist rechtskräftig.

d. Bescheid vom 21.4.2016, DSB-D122.451/0015-DSB/2016 (Auskunftsrecht gegenüber Versicherungsunternehmen, Anscheinsagent, Dienstleister)

Der Beschwerdeführer hatte mit einer ein Versicherungsunternehmen betreibenden Kapitalgesellschaft (Beschwerdegegnerin) einen Vertrag über eine Rechtschutzversicherung geschlossen. Der Vertrag kam über Vermittlung einer Ges.m.b.H. zustande, mit der der Beschwerdeführer einen Maklervertrag geschlossen hatte. Bei der Beschwerdegegnerin wurde die Ges.m.b.H. als „Betreuerin" des Beschwerdeführers geführt und hatte über ein Webportal Zugriff auf die vertragsbezogenen Daten des Beschwerdeführers. Nach einer Mahnung durch die interne Inkassoabteilung der Beschwerdegegnerin am 9. Oktober 2015 verlangte der Beschwerdeführer am 13. Oktober 2015 eine datenschutzrechtliche Auskunft. Diese wurde am 19. Oktober 2015 erteilt, worauf eine Beschwerde bei der Datenschutzbehörde wegen Inhaltsmängeln der Auskunft folgte. Die Datenschutzbehörde hielt in ihrem Bescheid fest, dass die Mahnung keine Zweckänderung der Datenverarbeitung und damit keine auskunftspflichtige Übermittlung war. Eine Speicherung der zur Korrespondenz mit der Beschwerdegegnerin verwendeten E-Mail-Adresse des Beschwerdeführers erfolgte nur innerhalb des E-Mail-Systems der Beschwerdegegnerin aufgrund der Beantwortung von dessen E-Mails. Diesbezüglich habe der Beschwerdeführer kein Rechtschutzinteresse an einer zusätzlichen Anführung seiner E-Mail-Adresse in einer Auskunft. Die Ges.m.b.H. sei auf Grundlage der Rechtsprechung zu versicherungsrechtlichen Vorschriften als „Anscheinsagent" und damit datenschutzrechtlich als

Dienstleister der Beschwerdegegnerin zu werten. Datenflüsse an die Ges.m.b.H. waren daher Datenüberlassungen. Da der Beschwerdeführer aber auch Auskunft über die Dienstleister der Beschwerdegegnerin verlangt und nicht erhalten hatte, wurde der Beschwerde nur in diesem Punkt rechtskräftig Folge gegeben.

e. Bescheid vom 12.5.2016, DSB-D122.468/0006-DSB/2016 (Auskunftsrecht gegenüber einem Handelsunternehmen, Unmöglichkeit der Auskunftserteilung)

Der Beschwerdeführer hatte sein Recht auf Auskunft gegenüber einer Ges.m.b.H. aus dem Handelsbereich (Beschwerdegegnerin) geltend gemacht (erst nach einer Beschwerde bei der Datenschutzbehörde wurde überhaupt Auskunft erteilt) und rügte nun in seiner Beschwerde (Folgeverfahren), dass die Beschwerdegegnerin keine Auskunft über die Herkunft seiner Daten erteilt habe. Die Beschwerdegegnerin wandte ein, dass keine Daten über die Herkunft der Daten des Beschwerdeführers gespeichert würden. Die Datenschutzbehörde stellte in ihrem Bescheid fest, dass nicht festgestellt werden konnte, woher die Daten des Beschwerdeführers stammen. Rechtlich sei das Recht auf Auskunft, auf die Auskunft über tatsächlich verarbeitete Daten beschränkt. Ist die Ermittlung der Herkunft von Daten infolge fehlender Dokumentation faktisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich, liegt keine Verletzung im Recht auf Auskunft vor, wenn die Herkunft der Daten nicht beauskunftet wird. Eine mögliche Verletzung der Protokollierungs- bzw. Dokumentationspflicht (§ 14 Abs. 2 Z 7 DSG 2000) oder des Rechts auf Geheimhaltung kann nicht im Beschwerdeverfahren nach § 31 Abs. 1 DSG 2000 geltend gemacht werden. Die Beschwerde wurde daher rechtskräftig abgewiesen.

f. Bescheid vom 12.5.2016, DSB-D122.515/0004-DSB/2016 (Auskunftsrecht gegenüber einem Dienstleister des AMS, Weiterleitungspflicht)

Der Beschwerdeführer verlangte von einem Dienstleister des Arbeitsmarktservice (AMS), bei dem er auf Aufforderung des AMS an „Auswahl-und Abklärungstagen" einschließlich eines elektronischen Intelligenz-Struktur-Tests teilgenommen hatte, Auskunft über die Daten des Testergebnisses. Der Dienstleister (Beschwerdegegner) verwies den Beschwerdeführer ans AMS. Die Datenschutzbehörde hielt in ihrem Bescheid fest, dass zwar der Dienstleister nicht selbst dem Beschwerdeführer die Auskunftserteilung schulde, er aber gemäß § 26 Abs. 10 DSG 2000 zur unverzüglichen Weiterleitung des eingelangten Auskunftsbegehrens an den Auftraggeber verpflichtet ist, damit der Auftraggeber in die Lage versetzt wird, innerhalb einer Frist von acht Wochen ab Einlangen des Auskunftsbegehrens beim Dienstleister auf das Auskunftsersuchen zu reagieren. Durch Missachtung dieser Bestimmung hat der Dienstleister selbst das Auskunftsrecht des Beschwerdeführers verletzt. Im Umfang dieser Feststellung wurde der Beschwerde rechtskräftig Folge gegeben.

g. Bescheid vom 29.6.2016, DSB-D122.436/0001-DSB/2016 (Auskunftsrecht gegenüber einem Krankenanstaltenbetreiber, Beschaffung von Informationen, Prozesssituation eines Dritten, nicht rechtskräftig)

Der anwaltlich vertretene Beschwerdeführer, der gegen ein Bundesland als Träger und Eigentümer einer Krankenanstalt einen Schadenersatzprozess führt, verlangte vom Betreiber der Krankenanstalt (Beschwerdegegner), einem öffentlich-rechtlichen Fonds, Auskunft über die zu seiner Person verarbeiteten Daten. In der anschließenden Beschwerde wegen Verletzung des Auskunftsrechts in Folge unvollständiger Auskunftserteilung brachte der Beschwerdeführer vor, der Beschwerdegegner habe ihm Auskunft über den ihn betreffenden Inhalt der E-Mail-Korrespondenz zwischen dem Beschwerdegegner und dessen Haftpflichtversicherung verweigert. Der Beschwerdegegner wandte dagegen ein, diese Daten wären gemäß § 26 Abs. 2 DSG

2000 aus überwiegenden berechtigten Interessen eines Dritten nicht zu beauskunften, weil dies die Prozesssituation des Landes in dem anhängigen Rechtsstreit um Schadenersatzansprüche des Beschwerdeführers schwächen könnte. Die Datenschutzbehörde folgte in ihrem Bescheid diesen Argumenten und wies die Beschwerde ab. Gegen diesen Bescheid ist Beschwerde an das Bundesverwaltungsgericht erhoben worden (anhängig zu Zl. W214 2132040-1).

h. Bescheid vom 15.7.2016, DSB-D122.453/0008-DSB/2016 (Auskunftsrecht gegenüber Privatperson, Videodokumentation von Flugbetrieb)

Der Beschwerdeführer verlangte als Betriebsleiter eines Hubschrauberlandeplatzes von einer Privatperson (Beschwerdegegner) unter Berufung auf § 50e DSG 2000 Auskunft über die Bilddaten einer behaupteten Videoüberwachung. Der Beschwerdegegner hatte immer wieder den Flugbetrieb gefilmt und wegen möglicher Verletzungen u.a. von luftfahrtrechtlichen Vorschriften Anzeigen an verschiedene Behörden erstattet. Die Auskunftserteilung gemäß § 50e DSG 2000 wurde vom Beschwerdegegner abgelehnt. Die Datenschutzbehörde stellte (u.a. nach Einsichtnahme in vom Beschwerdegegner vorgelegte MP4-Bilddateien) in ihrem Bescheid fest, dass der Beschwerdegegner nicht verantwortlicher Auftraggeber einer Videoüberwachung ist. Das anlassbezogene Filmen eines bestimmten Objekts von wechselnden Standorten aus mittels einer von Hand geführten Kamera zwecks Dokumentation von Ereignissen (hier: Flugbewegungen) und der Sicherung von Beweisen erfolgte hier nicht systematisch, insbesondere nicht mittels einer fest installierten Anlage, und auch nicht fortlaufend (§ 50a Abs. 1 DSG 2000). Daher kam dem Beschwerdeführer auch nicht das entsprechende Auskunftsrecht zu, die Beschwerde wurde rechtskräftig abgewiesen.

i. Bescheide vom 28.7.2016, DSB-D122.454/0006-DSB/2016 und 6.9.2016, DSB-D122.454/0010-DSB/2016 (Recht auf Geheimhaltung, personenbezogene Aktenzahl, Rechtsdokumentation durch ein Verwaltungsgericht, beide nicht rechtskräftig)

Im Verfahren Zl. DSB-D122.454, in dem zwei Teilbescheide ergangen sind, wandte sich der Beschwerdeführer wegen Verletzung seines Geheimhaltungsrechts gegen eine Salzburger Bezirksverwaltungsbehörde, das Amt der Landesregierung und das Landesverwaltungsgericht. Der Beschwerdeführer beanspruchte Leistungen der Mindestsicherung. Nach Vorgaben des Amtes der Landesregierung verwendete die Bezirksverwaltungsbehörde in entsprechenden Verfahren eine Aktenzahl, die das Geburtsdatum des Beschwerdeführers enthielt. Das Landesverwaltungsgericht dokumentierte ein Erkenntnis in einer den Beschwerdeführer betreffenden Sache zeitweilig auf seiner Website ohne Kürzung oder Weglassung dieser Aktenzahl. Die Datenschutzbehörde hielt fest, dass das Geburtsdatum ein personenbezogenes Datum ist, das für Zwecke der Aktenverwaltung einer – hier fehlenden – ausdrücklichen gesetzlichen Ermächtigung oder des – ebenfalls fehlenden – Nachweises bedarf, dass es sich bei der Verwendung des Geburtsdatums zur Bildung einer Aktenzahl um eine wesentliche Voraussetzung für die Wahrnehmung einer der Bezirksverwaltungsbehörde gesetzlich übertragenen Aufgabe handelt (§ 8 Abs. 3 Z 1 DSG 2000). Ob diese Form der Bildung einer Aktenzahl in irgendeiner Weise (etwa von einem hierarchisch übergeordneten (System-) Betreiber oder technisch durch den Softwarehersteller) vorgegeben war, war für die Frage der datenschutzrechtlichen Verantwortung nicht entscheidend. Diese Datenverwendung widerspricht den gesetzlichen Grundsätzen der Datensparsamkeit (Wesentlichkeit der Datenverwendung für den verfolgten Zweck) und des gelindesten Mittels. Der Beschwerde wurde daher (in einem Teilbescheid und nur gegenüber der Bezirksverwaltungsbehörde) Folge gegeben. Der Bescheid ist nicht rechtskräftig, da die Bezirksverwaltungsbehörde dagegen Amtsbeschwerde an das Bundesverwaltungsgericht erhoben hat. In einem zweiten Bescheid gab die Datenschutzbehörde der Beschwerde gegen die Präsidentin des Landesverwaltungsgerichts wegen Verletzung des Geheimhaltungsrechts

infolge unvollständiger Pseudonymisierung einer dokumentierten Entscheidung Folge. Die Datenschutzbehörde hielt hier fest, dass ihre Zuständigkeit gegeben war, da das Salzburger Landesverwaltungsgerichtsgesetz die Rechtsdokumentation samt Veröffentlichung in die Zuständigkeit der Präsidentin verweist und damit als Akt der Justizverwaltung und nicht als Akt der Gerichtsbarkeit definiert. Gegen diesen Bescheid wurde ebenfalls Amtsbeschwerde an das Bundesverwaltungsgericht erhoben.

3.2.2 Kontroll- und Ombudsmannverfahren

Im Kontroll- und Ombudsmannverfahren gemäß § 30 DSG 2000 kann sich jedermann wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten nach dem DSG 2000 mit einer Eingabe an die DSB wenden. Die Durchführung eines solchen weitestgehend formfreien Verfahrens ist (anders als beim Beschwerdeverfahren nach § 31 DSG 2000) unabhängig vom geltend gemachten Recht (Pflicht) oder dem angesprochenen Auftraggeber zulässig, und zwar auch dann, wenn die DSB alternativ auch zur förmlichen Rechtsdurchsetzung zuständig wäre. Ziel eines solchen Verfahrens ist nach § 30 Abs. 6 DSG 2000 die Herbeiführung des rechtmäßigen Zustands. Dazu kann die DSB, falls erforderlich, auch – nicht unmittelbar durchsetzbare – Empfehlungen aussprechen. Zumeist kann im Rahmen eines solchen Verfahrens eine datenschutzrechtlich zufriedenstellende Situation auch ohne Einsatz dieses Mittels erreicht werden.

Im Jahr 2016 betraf die zahlenmäßig größte Gruppe von Eingaben – nämlich eine Anzahl von 341 Eingangsstücken – Kontroll- und Ombudsmannverfahren, welche über Antrag eingeleitet wurden. Im Vergleich dazu wurden 90 Prüfungsverfahren amtswegig von der Datenschutzbehörde eingeleitet.

Im Berichtszeitraum scheinen des Weiteren die folgenden Fälle besonders erwähnenswert:

a. Im Rahmen ihrer Tätigkeit im Wettbewerbsschutz geht die Wirtschaftskammer Tirol durch die Abteilung „Wirtschaftsrecht, Steuerrecht und Umwelt (WSU)" Hinweisen auf Schwarzarbeit und illegale Gewerbetätigkeiten nach, weshalb Mitarbeiter dieser Abteilung Baustellen besichtigen, Fotos anfertigen und Personalien der angetroffenen Arbeiter erheben, um „Beweismittel" für eine allfällige Weiterleitung der erhobenen Informationen an die zuständigen Verfolgungsbehörden zu sichern. Informationen, die über ein verdächtiges Unternehmen erhoben wurden, werden auf Computern der Wirtschaftskammer Tirol gespeichert. Die Zulässigkeit einer solchen Ermittlung und Verarbeitung dieser Daten über gerichtliche und verwaltungsbehördlich strafbare Handlungen durch eine staatliche Behörde richtet sich dabei ausschließlich nach § 8 Abs. 4 DSG 2000. Die Wirtschaftskammer Tirol war der Ansicht, die gesetzliche Ermächtigung werde durch das Wirtschaftskammergesetz in seinen Bestimmungen §§ 1, 19, 43, 68 und 72 Abs. 1 geboten.

Die Datenschutzbehörde erkannte in seiner Entscheidung, dass § 72 Abs. 1 Wirtschaftskammergesetz zwar die Organisationen der gewerblichen Wirtschaft ermächtigt Daten im Sinne des Datenschutzgesetzes zu verwenden, wenn dies zur Erfüllung der ihnen gesetzlich aufgetragenen Aufgaben dient. Allerdings findet sich in dem in § 19 Abs. 1 Wirtschaftskammergesetz gesetzlich normierten Aufgabenbereich der Landeskammern nicht die Durchführung von Kontrollen von Unternehmern, um (verwaltungs)strafbare Handlungen wie Schwarzarbeit und illegale Gewerbetätigkeit aufzudecken. Auch beim Verweis auf den in § 43 Wirtschaftskammergesetz genannten – die in Rede stehende Befugnis ebenfalls nicht enthaltenden – Aufgabenkatalog, wurde übersehen, dass sich dieser ausschließlich auf die Tätigkeit der Fachgruppen bezieht. Bei der Fachgruppe einerseits und der Landeskammer andererseits handelt es sich aber um zwei verschiedene Körperschaften des öffentlichen Rechts und selbständige Wirtschaftskörper mit eigenem Wirkungsbereich. Auch der bloße Verweis der Wirtschaftskammer

Tirol auf § 68 Wirtschaftskammergesetz vermag keine geeignete Rechtsgrundlage aufzuzeigen, weil sich eine Amtshilfe immer nur auf Einzelfälle beziehen kann bzw. auch nicht dazu dienen soll, Handlungen zu verlangen, zu deren Vornahme keine gesetzliche Verpflichtung besteht. Eine gesetzliche Berechtigung zur Durchführung solcher Kontrollen und damit eine Ermächtigung zur Ermittlung und auch Speicherung dabei ermittelter Daten war daher nicht gegeben. Ein anderer Fall des § 8 Abs. 4 DSG 2000 war nicht erfüllt.

Die Datenschutzbehörde empfahl daher, die im Zuge von Baustellenkontrollen durch die Abteilung „Wirtschaftsrecht, Steuerrecht und Umwelt" der Wirtschaftskammer Tirol zum Zweck der Aufdeckung von Schwarzarbeit und illegaler Gewerbeausübung durchgeführte Ermittlung und Speicherung von Daten (Fotos und Personalien) möge zukünftig unterbleiben und die bisher auf diese Weise ermittelten und auf den Computern der Wirtschaftskammer Tirol gespeicherten Daten sind zu löschen.

b. Empfehlung wegen Ermittlung, Speicherung und Übermittlung personenbezogener Daten im Eingangsbereichs eines Lokals (DSB-D215.865/0011.DSB/2016, 1. Dezember 2016).

Die Einschreiterin machte geltend, dass der Erstbelangte, als Anrainer des von der Einschreiterin betriebenen, ca. 25 Meter entfernt liegenden Lokals jedes Wochenende in der Nachtzeit den Bereich vor dem Lokal laufend fotografieren würde, um die Fotodokumentation an verschiedene Politiker und Behörden zu versenden. Dieses Vorgehen stelle laut der Einschreiterin eine rechtswidrige Videoüberwachung im Sinne des § 50a DSG 2000 oder eine rechtwidrige Verwendung von Daten dar.

Die Datenschutzbehörde berücksichtigte in ihrer Entscheidung, dass zwar den erläuternden Bemerkungen zur Regierungsvorlage der DSG-Novelle 2010 zu entnehmen ist, dass auch „gezieltes Fotografieren" eine Videoüberwachung darstellen kann, jedoch ist hierfür ein intentional auf die Überwachung eines Objekts oder einer Person gerichtetes Verhalten erforderlich. Dem gegenüber sind „Fall zu Fall Aufnahmen" – etwa um anlassbezogen „Belege" für Verwaltungsübertretungen zu erhalten, mögen diese auch zahlreich und häufig aufgenommen worden sein – nicht als Videoüberwachung im Sinne des § 50a Abs. 1 DSG 2000 zu qualifizieren. Die Ermittlung personenbezogener Daten samt Beigabe von Beweismitteln zur Erstattung einer Anzeige an eine zur Verfolgung der angezeigten strafbaren Handlungen (Unterlassungen) zuständige Behörde findet in § 8 Abs. 4 Z 4 DSG 2000 Deckung, wobei nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen verstoßen wird, wenn die Datenweitergabe zum Zweck der Anzeigenerstattung an die zuständige Behörde erfolgt und überdies auf das unbedingt notwendige Ausmaß beschränkt bleibt (§ 1 Abs. 2 letzter Satz DSG 2000). Im gegenständlichen Fall enthielten die den Anzeigen, Eingaben und Beschwerden beigefügten Fotos eine teils zeitlich ausgesprochen verdichtete Frequenz – Aufnahmen im Sekunden- und Minutentakt – deren denkbarer Zweck auch aus Gründen der Beweissicherung nicht ersichtlich war.

Daher empfahl die Datenschutzbehörde, der Erstbelangte möge die Ermittlung, Speicherung und Übermittlung von personenbezogenen Daten des Eingangsbereichs des Lokals, zum Zwecke des Beweises von behaupteten Verwaltungsübertretungen durch Fotos oder Videosequenzen von identifizierbaren Personen (etwa Passanten) oder Kennzeichen von Kraftfahrzeugen (jeweils vom öffentlichen Raum angefertigt) auf jenes Ausmaß beschränken, wie es für den Zweck der Erstattung einer Anzeige für die jeweilige Verwaltungsübertretung an die zuständige Behörde erforderlich ist.

c. Empfehlung zur unzulässigen Ermittlung von Daten aus dem Gesamtverzeichnis des R***-Verbandes (DSB-D216.175/0004-DSB/2016), 7. Dezember 2016)

Die datenschutzrechtliche Auftraggeberin versandte im September 2015 im Rahmen der Gemeinderatswahl Wien zwei Wahlwerbungsschreiben an den Einschreiter. In der Anrede gegenständlicher Schreiben wurden die im Rahmen des Verbandes verwendeten „Couleurnamen" des Einschreiters benutzt. Dafür wurden folgende Daten der Mitglieder des R***-Verbandes aus dem Gesamtverzeichnis des R***-Verbandes ermittelt: Anrede, Akademischer Grad, Vorname, Nachname, Adresszusatz, Straße, Postleitzahl, Ort, Land, Geburtsdatum sowie der Couleurname. Diese Daten wurden mit den Daten aus der Wählerliste abgeglichen und wahlberechtigte Mitglieder, darunter auch der Einschreiter, zur Unterstützung angeschrieben.

Die DSB verwies darauf, dass eine Berechtigung zur Ermittlung von (in der Wählerevidenz allenfalls nicht enthaltenen) Daten (wie zB. Couleurname) zum Zweck der Wahlwerbung nicht ohne weiteres aus § 1 Abs. 2 PartG abgeleitet werden darf. Wenngleich diese Bestimmung festlegt, dass es zu den Aufgaben der Antragsgegnerin als politische Partei zählt, an der politischen Willensbildung mitzuwirken und damit Daten (Name und Anschrift) aus der (auch) den politischen Parteien zur Verfügung stehenden und zu Wahlzwecken geführten Wählerevidenz für Zwecke der Wahlwerbung verwenden zu dürfen. Beim R***-Verband handelt es sich um einen Schüler- und Absolventen Verband Österreichs, dessen Hauptanliegen die Mitgestaltung der Schulpolitik im Interesse der Schüler ist. Das die Mitglieder enthaltende Gesamtverzeichnis des R***-Verbandes steht ausschließlich Mitgliedern, und damit nicht jedermann zur Verfügung. Die Antragsgegnerin war als politische Partei nicht Mitglied des R***-Verbandes und als solche daher zur Verwendung von Daten aus dem Gesamtverzeichnis gemäß § 7 Abs. 1 DSG 2000 nicht berechtigt. Die DSB empfahl eine zum Zweck der Aussendung von Wahlwerbungen der Antragsgegnerin erfolgte Ermittlung von Daten aus dem Gesamtverzeichnis der R***-Verbandes möge zukünftig unterbleiben.

3.2.3 Rechtsauskünfte an Bürgerinnen und Bürger

Die Datenschutzbehörde stellt auf ihrer Homepage umfassende Rechtsinformationen in Zusammenhang mit dem DSG 2000 zur Verfügung https://www.dsb.gv.at/fragen-und-antworten. Diese umfassen, gut verständlich und an der Praxis orientiert, Antworten auf die relevantesten datenschutzrechtlichen Themen und häufigsten Fragen. Weiters werden auf der Homepage ausführliche Rechtsinformationen über die Rechte der Betroffenen und die Verfahrensarten nach dem DSG 2000 zur Verfügung gestellt https://www.dsb.gv.at/rechte-der-betroffenen. Darüber hinaus beantwortet die Datenschutzbehörde auch allgemeine Anfragen zum Datenschutz schriftlich. Telefonische Rechtsauskünfte werden nicht erteilt.

Die Datenschutzbehörde nimmt im Rahmen einer Rechtsauskunft keine auf den Einzelfall bezogene inhaltliche rechtliche Beurteilung vor. Diese rechtlichen Beurteilungen können auf Grund der gesetzlichen Zuständigkeit der Datenschutzbehörde nur im Zuge eines konkreten Verfahrens vorgenommen werden. Jede Vorabbeurteilung würde das Ergebnis eines allfälligen Verfahrens vor der Datenschutzbehörde vorwegnehmen.

3.2.4 Genehmigungen im Internationalen Datenverkehr

Im Berichtszeitraum gab es im Bereich des Internationalen Datenverkehrs, den Genehmigungsverfahren zum Export personenbezogener Daten gemäß § 13 DSG 2000, einige neue Entwicklungen.

Im Jahr 2016 kam es beinahe zu einer Verdreifachung des Aktenanfalls im Vergleich zu 2015. Die Datenschutzbehörde begegnet dieser Herausforderung mit mehreren Maßnahmen. Die Fäl-

le werden auf drei juristische SachbearbeiterInnen aufgeteilt; darüber hinaus werden nicht-juristische Sachbearbeiterinnen in diese Arbeit eingebunden. Diese Schritte tragen zur zeitnahen Erledigung der Anträge gemäß § 13 DSG 2000 bei.

Die Datenschutzbehörde hat eine „Checkliste für Anträge im internationalen Datenverkehr gemäß § 13 DSG 2000" erarbeitet, die auf der Website der Datenschutzbehörde auf der Seite „Dokumente" abrufbar ist (https://www.dsb.gv.at/dokumente). Die Checkliste soll eine Hilfestellung für Antragsteller darstellen und die Zahl der durch die DSB zu erteilenden Mangelbehebungsaufträge auf einen einzigen reduzieren.

Ein weiteres Ereignis war die Neuregelung des Datenverkehrs mit den USA. Die Weitergabe von personenbezogenen Daten in die USA war bis zum Oktober 2015 unter bestimmten Bedingungen genehmigungsfrei. Diese Regelung trug die Bezeichnung „Safe Harbor" (2000/520/EG). Als der Europäische Gerichtshof am 6. Oktober 2015, C-362/14, die Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärte, fiel diese Ausnahme weg.

Am 12. Juli 2016 hat die Europäische Kommission mit dem Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes („EU-US Privacy Shield") eine neue Regelung angenommen. Wie bei der alten „Safe Harbor"-Regelung wirkt der Beschluss nicht für das gesamte Land, sondern nur für Datenempfänger, die sich vom US-Handelsministerium (U.S. Department of Commerce) zertifizieren lassen und auf einer Liste der Mitglieder aufscheinen.

Die Mitgliedschaft beim EU-US Privacy Shield muss für jeden Empfänger von der Behörde anhand der im Internet veröffentlichten Liste überprüft werden (www.privacyshield.gov/list). Die Datenschutzbehörde hat die Beobachtung gemacht, dass die Antragssteller diese Liste offenbar selten konsultieren und auch die eingetragenen Unternehmen ihr Recht, Daten genehmigungsfrei zu empfangen, wenig kommunizieren. In manchen internationalen Konzernen wird offenbar auch lückenhaft informiert, dass ein Empfänger im Konzernverband das Privileg des EU-US Privacy Shields in Anspruch nehmen kann. Die Behörde hat mehrfach Antragssteller darauf hingewiesen, dass ein Empfänger in den USA unter die Regelung des EU-US Privacy Shield fällt und daher keine Genehmigung erforderlich ist.

3.2.5 Entscheidungen im Registrierungsverfahren

Registrierungen:

a. Registriert wurde die seitens der ÖBB-Infrastruktur AG gemeldete Datenanwendung „Anlassbezogener Einsatz von Videoüberwachung („BodyCams") zur Dokumentation von kritischen Situationen durch Sicherheitsmitarbeiter der Auftraggeberin". Es handelt sich dabei um am Körper getragene Kameras, welche gut sichtbar zwischen Schulter- und Brustbereich angebracht sind. Zweck ist u.a. die Stärkung des Sicherheitsgefühls der Fahrgäste und eine gewisse Präventionswirkung, um Übergriffe auf das Personal zu reduzieren. Diese Videokameras dürfen, wie auch im Falle von herkömmlichen Videoüberwachungsanlagen, nur in jenen Bereichen eingesetzt werden, über welche die Auftraggeberin verfügungsbefugt ist (d.h. eigene Liegenschaften und Gebäude, insbesondere öffentliche Verkehrsstationen). Dabei wird die Aufnahme gegebenenfalls - also insbesondere bei Verdacht auf einen strafrechtlich relevanten Vorfall - manuell ausgelöst. Betroffene werden vor dem Aktivieren der Aufzeichnungen ausdrücklich darüber in Kenntnis gesetzt. Eine optische Kennzeichnung dieser anlassfallbezogenen Videoüberwachung erfolgt auf den Sicherheitswesten der Mitarbeiter (Piktogramm einer Videokamera oder Aufschrift „VIDEO"), und durch ein Blinklicht an der Kamera selbst. Zusätzlich wird durch ein akustisches Signal auf das

Auslösen der Aufzeichnung aufmerksam gemacht. In höchstpersönlichen Lebensbereichen (WC-Anlagen, Umkleideräumlichkeiten etc.) darf kein Einsatz dieser Kameras erfolgen. Tonaufzeichnungen finden keine statt.

b. Ebenso wurde eine Datenanwendung mit der Bezeichnung „Offener Einsatz von Bild- und Tonaufzeichnungsgeräten gemäß § 13a (3) SPG zur Dokumentation von Amtshandlungen, bei denen Organe des öffentlichen Sicherheitsdienstes Befehls- und Zwangsgewalt ausüben" registriert. Ihr Zweck ist die Ermittlung personenbezogener Daten von Personen mit Bild- und Tonaufzeichnungsgeräten durch Organe der Landespolizeidirektion Wien zur Dokumentation von Amtshandlungen, zur Verfolgung von strafbaren Handlungen sowie zur Kontrolle der Rechtmäßigkeit der Amtshandlung. Vor Beginn der Aufzeichnung wird der Einsatz der Kamera mündlich angekündigt. Das Aufzeichnungs- und Auswertungssystem ist verschlüsselt. Hierfür besteht mit § 13a Abs. 3 Sicherheitspolizeigesetz eine ausdrückliche gesetzliche Ermächtigung.

c. Registrierungen von Meldungen über die Datenverwendung im Zuge des Bankenpakets, welche von Auftraggebern (über 600 Bankinstitute) aufgrund der Verpflichtungen u.a. des Kontenregister- und Konteneinschaugesetzes sowie des Kapitalabfluss-Meldegesetzes eingebracht wurden. Das Datenverarbeitungsregister stellte hierfür über DVR-ONLINE ein gemeinsam mit dem Bundesministerium für Finanzen ausgearbeitetes Ausfüllmuster zur Verfügung.

d. Registriert wurde ein vom Verband der Versicherungsunternehmen Österreichs (VVO) betriebenes Informationsverbundsystem mit der Bezeichnung „Zentrales Informationssystem der österreichischen Versicherungswirtschaft im Bereich der Kranken- und Lebensversicherung". Teilnehmende Auftraggeber an diesem System sind konzessionierte und zum Geschäftsbetrieb befugte Versicherungsunternehmen. Die Registrierung erfolgte aufgrund der Zusage folgender Auflagen:

„Jede der in der Registrierung aufgelisteten Auftraggeberinnen sagt für ihre Teilnahme am „Zentralen Informationssystem der österreichischen Versicherungswirtschaft im Bereich der Kranken- und Lebensversicherung", welches ein Informationsverbundsystem im Sinne des § 50 DSG 2000 darstellt, gemäß § 19 Abs. 2 DSG 2000 die Einhaltung der folgenden Auflagen zu:

1. In das Informationssystem werden versicherte und zu versichernde Personen nur dann eingetragen, wenn ein Antrag auf Versicherungsabschluss auf Dauer oder vorübergehend abgelehnt wird, potentiell zu erschwerten Bedingungen angenommen wird oder angenommen worden wäre, wenn eine Berufsunfähigkeitsversicherung mit Rentenbezug abgeschlossen wird, bei welcher die versicherte Jahresrente auch unter Berücksichtigung allfälliger Vorverträge mehr als EUR 9.000 beträgt und bei vorzeitiger Beendigung des Versicherungsvertrags durch das Versicherungsunternehmen aufgrund einer festgestellten oder vermuteten Verletzung der vorvertraglichen Anzeigepflicht. Die Eintragungen in das System erfolgen nach einheitlichen und objektivierbaren Kriterien. Hierfür verfügt jeder Auftraggeber über entsprechende Vorgaben und Handbücher.

2. Jedes am Informationssystem teilnehmende Versicherungsunternehmen informiert gemäß § 24 Abs. 2 Z 3 DSG 2000 im Antragsformular in einem separierten und schriftvergrößerten Feld über das Bestehen des Informationssystems und über die Möglichkeit der Einspeicherung der zu versichernden Person in dieses System. Die Information enthält die Voraussetzungen und Gründe der Einspeicherung in das Informationssystem und sie erklärt, welche Daten der zu versichernden Person in das System eingetragen werden. Sie erklärt auch, dass für die zu versichernde Person bereits mit Unterfertigung des Antrags die potentielle Möglichkeit der Einspeicherung in das Informationssystem besteht, somit auch wenn der Betroffenen seinen Antrag von sich aus zurückziehen sollte. Es erfolgt keine Eintragung eines Betroffenen, ohne

dass dieser zuvor eine Unterschrift geleistet hat (etwa im Zuge eines Antrages bzw. eines Vertragsabschlusses).

3. Wird ein Betroffener in das Informationssystem eingemeldet, so wird dieser im Rahmen der hierbei anfallenden Korrespondenz in jedem Fall gemäß § 24 Abs. 2 Z 3 DSG 2000 von der erfolgten Eintragung informiert.

4. Die Identität des Versicherungsunternehmens, welches die Einmeldung veranlasst hat, ist nur für den VVO als Systembetreiber ersehbar. Nur im Fall eines berechtigten Interesses eines Versicherungsunternehmens an der Kenntnis des einmeldenden Versicherungsunternehmens, um einem auf diese Beauskunftung abzielenden Auskunftsbegehren einer versicherten oder zu versichernden Person entsprechen zu können oder in wertungsgleichen Fällen (etwa in anhängigen Gerichtsverfahren) - somit ausschließlich in Fällen, in denen eine Bevollmächtigung durch den Betroffenen bzw. ein entsprechender gerichtlicher oder behördlicher Beschluss vorliegt - legt der VVO diesem Versicherungsunternehmen die Identität des einmeldenden Versicherungsunternehmens offen.

5. Die Eintragungen in das Informationssystem bleiben längstens sieben Jahre bestehen. Eine Bestreitung der Richtigkeit einer Eintragung im Informationssystem wird unmittelbar durch einen Bestreitungsvermerk ersichtlich gemacht.

6. Die teilnehmenden Versicherungen schließen mit dem VVO als Systembetreiber einen Betreibervertrag über den Betrieb des Informationssystems.

7. Jedes teilnehmende Versicherungsunternehmen verfügt über ein eigenes Kompetenzzentrum, welches Aufgaben im Zusammenhang mit dem Informationssystem (Erstellung von Einmelde-Richtlinien, Mitarbeiterschulungen etc.) wahrnimmt."

Ablehnungen/Zurückweisungen im Registrierungsverfahren:

a. Seitens einer österreichischen Flughafenbetriebsgesellschaft wurde die geplante Videoüberwachung eines Teilabschnitts einer Bundesstraße gemeldet. Dabei handelte es sich im Wesentlichen um jenen Teil der Bundesstraße, der in Form einer Unterführung unter einer Landebahn des Flughafens hindurchführt. Diese Unterführung wurde immer wieder durch zu hohe LKWs beschädigt. Die Auftraggeberin ist aufgrund einer grundbücherlichen Eintragung berechtigt, auf dem Gelände oberhalb der Bundesstraße eine Start- und Landebahn zu betreiben. Da die dingliche Berechtigung eines Auftraggebers zwar grundsätzlich eine ausreichende Verfügungsbefugnis zur allfälligen Überwachung seines eigenen Bauwerkes bzw. seines eigenen Geländes darstellt, jedoch nicht die Befugnis zum Einsatz von Videoüberwachung auf angrenzenden, in diesem Fall darunter hindurchführenden, öffentlichen Straßen umfasst, wurde die Registrierung abgelehnt. Anzumerken ist, dass auch der Grundeigentümer bzw. der zuständige Straßenerhalter ohne spezielle gesetzliche Rechtsgrundlage (etwa in der StVO) ebenfalls nicht berechtigt wären, eine derartige Überwachung des öffentlichen Verkehrs durchzuführen.

b. Die Meldung einer als „Video Event Data Recorder" (vergleichbar mit einer Dash-Cam in Fahrzeugen) bezeichneten Datenanwendung eines Unternehmens mit Sitz in Italien wurde wegen Unzuständigkeit der Datenschutzbehörde bescheidmäßig zurückgewiesen. Da die Meldungslegerin über keine Niederlassung in Österreich verfügt, ist gemäß § 3 Abs. 2 DSG 2000 das Recht des Sitzstaates auf die geplante Datenverarbeitung anzuwenden, nicht jedoch das Österreichische Datenschutzgesetz 2000. Eine rechtliche Beurteilung der Zulässigkeit der gegenständlichen Datenanwendung hat somit in Italien zu erfolgen.

3.2.6 Stammzahlenregisterbehörde

Allgemeines

Hinter vielen elektronischen Formularen und von öffentlichen Einrichtungen betriebenen Registern andere Dienstleistungen, die mit der Bürgerkarte oder Handysignatur sicher genutzt werden können, stecken von der Datenschutzbehörde betriebene Datenanwendungen. Ein datenschutzfreundliches System zur eindeutigen Identifizierung von Personen (das Stammzahlenregister), ein Personenregister für Personen, die nicht im zentralen Melderegister einzutragen sind (das Ergänzungsregister für natürliche Personen), das größte österreichische Unternehmensregister in dem alle Unternehmen erfasst werden können, die nicht im Firmenbuch oder Vereinsregister einzutragen sind (das Ergänzungsregister für sonstige Betroffene) und ein Register das vertretungsweises Handeln mittels Bürgerkarte oder Handysignatur ermöglicht (das Vollmachtenregister)

Zahlen und Überblick

Stammzahlenregister

Im Jahr 2016 wurden über 200 Millionen bereichsspezifische Personenkennzeichen (bPK) berechnet. Das entspricht einer Steigerung von 50% im Verhältnis zum Jahr davor. Verantwortlich dafür sind vor allem die Erstausstattungen der Kreditinstitute zum Zweck der Meldung in das Kontenregister[1]. Die damit verbundenen Umsetzungsmaßnahmen haben sowohl bei der Datenschutzbehörde als auch bei ihren Dienstleistern Mehrarbeit in diesem Bereich erforderlich gemacht.

Vollmachtenregister

Zwischen 2011 und 2016 wurden 2.814 Vollmachten in das Vollmachtenregister eingetragen. 2016 wurden 479 neue Vollmachten eingetragen. In Vertretung gehandelt wurde 17.805 Mal. Berufsmäßige Parteienvertreter haben das Service 3.057 Mal benutzt.

Ergänzungsregister für natürliche Personen

2016 wurden 62.931 Transaktionen im Ergänzungsregister für natürliche Personen (Neuanlagen, Änderungen, Beendigungen) durchgeführt. 38.960 davon waren Eintragungen neuer Personen in das Register. Insgesamt waren zum Stichtag 31.12.2016 182.275 Personen eingetragen.

Ergänzungsregister für sonstige Betroffene :

2016 enthielt das Register 1.417.989 aktive und 352.604 inaktive Unternehmen. 132.458 Neueintragungen und 600.172 Änderungen wurden vorgenommen. Das Register wurde 352.678 Mal über die Weboberfläche abgefragt und 20.626.451 Mal von Behörden über die zur Verfügung gestellte Schnittstelle durchsucht.

1 Mit dem Bundesgesetz über die Einrichtung eines Kontenregisters und die Konteneinschau (Kontenregister- und Konteneinschaugesetz – KontRegG) StF: BGBl. I Nr. 116/2015 wurde im Finanzministerium ein Register geschaffen, in dem alle Kontoinhaber bei den österreichischen Kreditinstituten erfasst werden (näheres dazu weiter unten unter der Überschrift „Entwicklungen" und „Bankenpaket", „Spendenpaket").

Die Aufgaben und Datenanwendungen der Stammzahlenregisterbehörde

Erzeugung von bereichsspezifischen Personenkennzeichen

Im E-Government-System erfolgt die eindeutige Identifikation von natürlichen Personen durch eine geheime Stammzahl und davon abgeleiteten bereichsspezifischen Personenkennzeichen (bPK). Die Stammzahl darf nur auf der Bürgerkarte gespeichert werden. Sie wird aus der im zentralen Melderegister verwendeten ZMR-Zahl mit Hilfe eines geheimen Schlüssels gebildet. Der geheime Schlüssel und alle damit verknüpften Funktionen werden von der DSB in ihrer Funktion als Stammzahlenregisterbehörde verwaltet.

Die Stammzahlenregisterbehörde erzeugt bereichsspezifische Personenkennzeichen (bPK), stellt Anwendungen zur Erzeugung von bereichsspezifischen Kennzeichen auf Grundlage der Stammzahl zur Verfügung und stellt sicher, dass diese richtig eingesetzt werden. Zu diesem Zweck müssen Auftraggeber des öffentlichen Bereichs einen Antrag bei der Stammzahlen-registerbehörde auf Erlaubnis der Ausstattung einer Datenanwendung mit bPK stellen. Ein bereichsspezifisches Personenkennzeichen kann weder auf die Stammzahl zurückgerechnet werden, noch – ohne zusätzliche Angaben über die Person und der Mitwirkung der Stammzah¬lenregisterbehörde – in ein bereichsspezifisches Personenkennzeichen eines anderen Bereichs umgerechnet werden.

Das erleichtert der öffentlichen Verwaltung die Zuordnung von Personen zu Verfahren, erlaubt es den betroffenen Bürgern mit einem einzigen sicheren Mechanismus öffentliche Dienstleis¬tungen bequem elektronisch abzuwickeln und schützt gleichzeitig die Betroffenen vor einer leichteren Zusammenführbarkeit ihrer Daten. Sichergestellt wird insbesondere, dass es durch die eindeutige elektronische Identifizierung zu keiner einfachen Zusammenführbarkeit der mit bPK verknüpften Daten kommen kann, indem die bPK für verschiedene Bereiche der öffentlichen Verwaltung anders gebildet werden. Dadurch sind diese Kennzeichen in Datenanwendungen eines anderen Bereichs unbrauchbar.

Ergänzungsregister

Die DSB betreibt zwei „Ergänzungs"register, in die sich jene natürlichen Personen und sonstige rechtlich erhebliche Entitäten eintragen lassen können, die in keinem der Basisregister des E-Government-Systems eingetragen sind.

In das Ergänzungsregister für natürliche Personen (ERnP) können Personen eingetragen werden, die nicht im zentralen Melderegister eingetragen werden müssen.

In das Ergänzungsregister für sonstige Betroffene (ERsB) kann jedes Unternehmen eingetragen werden, das nicht im Firmenbuch oder Vereinsregister erfasst werden muss (z.B. Behörden, Religionsgemeinschaften oder Arbeitsgemeinschaften). Unternehmen und juristische Personen werden im österreichischen E-Government mit bereichsübergreifenden Kennzeichen, die zum Teil auch offen (Firmenbuchnummer) geführt werden, identifiziert. Diese Kennzeichen werden in E-Government Anwendungen als Stammzahl verwendet. Das Ergänzungsregister für sonstige Betroffene schließt die Lücke für jene Unternehmen, die in Österreich kein Kennzeichen haben.

Vollmachtenregister

Das Vollmachtenregister erlaubt vertretungsweises Handeln in E-Government Anwendungen von Personen, deren Einzelvertretungsbefugnis in einem Basisregister des E-Government-Systems (Firmenbuch, Ergänzungsregister für sonstige Betroffene oder Vereinsregister) eingetragen wurde oder durch Ausstellung einer Vollmacht mittels Bürgerkarte oder Handysignatur und Übertragung auf die Bürgerkarte oder Handysignatur einer anderen Person. In diesem

Zusammenhang weist die DSB auf das vom Bundesministerium für Finanzen betriebene Unternehmensserviceportal (USP) hin, das Unternehmen eine ähnliche Funktionalität anbietet.

Entwicklungen

a. Milliardengrenze bei bPK Ausstellung überschritten

In ihrem 12jährigen Bestehen hat die Stammzahlenregisterbehörde mehr als eine Milliarde bPK im Rahmen der Erst- und Folgeausstattung ausgestellt und bewältigt derzeit etwa 3,3 Millionen Abfragen monatlich über die zur Verfügung gestellten Schnittstellen. Insgesamt waren Ende 2016 182.275 Personen im ErNP und 1.417.989 Personen im ERsB eingetragen.

b. „Bankenpaket", „Spendenpaket"

Das Jahr 2016 stand für die Stammzahlenregisterbehörde im Zeichen der Umsetzung des Bankenpaketes und der Planung, Vorbereitung und Entwicklung technischer Konzepte für die Umsetzung des Spendenpaketes.

b.1 Bankenpaket

Am 14. August 2015 wurde in BGBl. I 2015 / 116 das sogenannte „Bankenpaket" kundgemacht, mit dem unter anderem das Kontenregister- und Konteneinschaugesetz (KontRegG), sowie das Bundesgesetz über die Meldepflicht von Kapitalabflüssen und von Kapitalzuflüssen (Kapitalabfluss-MeldeG) beschlossen wurde[2]. Mit 1. August 2016 erfolgte in BGBl. I 2016/77 die Kundmachung einer Novellierung sowohl des Kontenregister- und Konteneinschaugesetzes (KontRegG) als auch des Bundesgesetzes über die Meldepflicht von Kapitalabflüssen und von Kapitalzuflüssen (Kapitalabfluss-MeldeG)[3].

In § 4 Abs. 1 der Kontenregister-Durchführungsverordnung (KontReg-DV) des Bundesministers für Finanzen vom 26. April 2016 wurde festgelegt, dass eine Abfrage des Kontenregisters für Berechtigte bereits mit 5. Oktober 2016 möglich sein sollte, sodass eine rasche Umsetzung geboten war.

Sowohl im Kontenregister (§ 2 Abs. 1 des KontRegG) als auch bei Meldungen über Kapitalabflüsse (§ 3 Abs. 3 Kapitalabfluss-MeldeG) ist vorgesehen, dass das bereichsspezifische Personenkennzeichen für Steuern und Abgaben (bei natürlichen Personen als Kunden) oder die Stammzahl (bei Rechtsträgern als Kunden) in das Kontenregister einzutragen oder in die Meldung über Kapitalabflüsse aufzunehmen ist.

Zur Erzeugung der bereichsspezifischen Personenkennzeichen oder Stammzahlen ist gemäß § 10 Abs. 2 E-GovG die Stammzahlenregisterbehörde berufen, wobei sich die Stammzahlenregisterbehörde bei der Errechnung von „bPK" des Bundesministeriums für Inneres als Dienstleister (soweit natürliche Personen Betroffene sind) und der Bundesanstalt Statistik Österreich hinsichtlich aller anderen Betroffenen bedienen kann.

2 https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2015_I_116/BGBLA_2015_I_116.pdf
3 https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2016_I_77/BGBLA_2016_I_77.pdf

Die Umsetzung des Bankenpaketes brachte sowohl in inhaltlicher als auch in zeitlicher Hinsicht erhebliche Herausforderungen für die Stammzahlenregisterbehörde und ihre technischen Dienstleister (Bundesministerium für Inneres und Statistik Austria. mit sich.

So mussten die technischen und organisatorischen Voraussetzungen für eine „vertretungsweise" Übermittlung von Datensätzen zur Ausstattung mit bPK und Stammzahlen durch die zahlreichen technischen Dienstleister der Banken (Rechenzentren der Banken) geschaffen werden. Es waren neue Formulare für den Antrag auf Erstausstattung durch die Kreditinstitute zu erstellen, sowie ein Ausfüllmuster für die Meldung der Datenanwendung „Bankenpaket" beim Datenverarbeitungsregister gemeinsam mit den Vertretern der Banken zu erarbeiten. Die zahlreichen technischen Fragen der Kreditinstitute und ihrer Dienstleister sowie die Antworten wurden im sogenannten „UBIT-Forum" der Wirtschaftskammer veröffentlicht, sodass eine effiziente und zeitgleiche Kommunikation für alle teilnehmenden Kreditinstitute gewährleistet war.

Da die Stammzahlenregisterbehörde bei der Befüllung des Kontenregisters im chronologischen Ablauf die erste Anlaufstelle bildete, war eine enge und verzahnte Zusammenarbeit mit den federführenden Abteilungen im Finanzressort, sowie ein regelmäßiges reporting über den „Ausstattungsfortschritt" ein zentraler Schlüssel für den Erfolg des Projekts. Das Kontenregister ging mit 5.Oktober 2016 in Betrieb.

Im Jahr 2016 wurden im Rahmen des Bankenpaketes 83.242.074 Datensätze für 640 Banken verarbeitet. Insgesamt wurden 21.877 Datenübermittlungen über das BMI abgewickelt, 8.713 für die Statistik Austria und 13.164 für das Stammzahlenregister.

b.2 Spendenpaket

Am 14. August 2015 wurde in BGBl. I 2015 / 118[4] das „Steuerreformpaket 2015/16" kundgemacht, mit dem unter anderem veränderte Regelungen im Einkommensteuergesetz 1988 betreffend der Berücksichtigung von Beiträgen (etwa Beiträge im Rahmen der Weiterversicherung in der gesetzlichen Pensionsversicherung, Kirchenbeitrag) und Zuwendungen (etwa Spenden) als Sonderausgaben beschlossen wurden. Demnach sind Beiträge gemäß § 18 Abs. 1 Z 1a und Z 5 EStG 1988 idgF sowie für Zuwendungen gemäß § 18 Abs. 1 Z 7 bis 9 leg. cit. an einen Empfänger, der eine feste örtliche Einrichtung im Inland unterhält, nur dann als Sonderausgaben zu berücksichtigen, wenn dem Empfänger Vor- und Zunamen und das Geburtsdatum des Leistenden bekannt gegeben werden und eine Datenübermittlung erfolgt. Mit Kundmachung vom 30.12.2016 in BGBl I, Nr.117/2016 wurde u.a. eine Novellierung des § 18 Abs. 8 EStG 1988 idgF kundgemacht, wonach Datenanwendungen auf Grundlage der § 18 Abs. 8 Z 1 bis 3 EStG 1988 idgF von der Meldepflicht gemäß § 17 Abs. 1 DSG 2000 ausgenommen wurden[5].

Nähere Informationen dazu unter folgendem Link zur Webseite des BMF:
https://www.bmf.gv.at/kampagnen/spendenservice.html#Steuerliche_Absetzbarkeit_von_Spenden

Informationsfolder des BMF:
https://www.bmf.gv.at/steuern/BMF-BR-ST_Spendenabsetzbarkeit_122016_web.pdf?5s3qah

4 https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2015_I_118/BGBLA_2015_I_118.pdf
5 https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2016_I_117/BGBLA_2016_I_117.pdf

Gemäß § 18 Abs. 8 lit. a EStG 1988 idgF sind von den Zuwendungsempfängern (also beispielsweise Spendenorganisationen) das verschlüsselte bereichsspezifische Personenkennzeichen für Steuern und Abgaben (vbPK SA. des Leistenden, wenn dieser dem Empfänger Vor- und Zunamen und sein Geburtsdatum bekannt gegeben hat, und der Gesamtbetrag aller im Kalenderjahr zugewendeten Beträge des Leistenden an das Bundesministerium für Finanzen zu übermitteln.

In § 14 Abs. Z 2 der Sonderausgaben-Datenübermittlungsverordnung[6] des Bundesministers für Finanzen vom 24. Oktober 2016 wurde festgelegt, dass Daten, die übermittelte Zuwendungen betreffen, im Rahmen der automatisationsunterstützten Datenverarbeitung nur summarisch und ohne Benennung der jeweils übermittelnden Organisation zugänglich gemacht werden, soweit die übermittelten Zuwendungen nicht Gegenstand einer konkreten Überprüfungshandlung sind. Der Gesamtbetrag der von der Datenübermittlung betroffenen Zuwendungen ist nach Kategorien gegliedert darzustellen.

Zur Erzeugung der bereichsspezifischen Personenkennzeichen ist gemäß § 10 Abs. 2 E-GovG die Stammzahlenregisterbehörde berufen, wobei sich die Stammzahlenregisterbehörde bei der Errechnung von „vbPK" des Bundesministeriums für Inneres als Dienstleister bedienen kann. Da im Rahmen des „Spendenpakets" gemäß § 18 Abs. 8 lit. a EStG 1988 idgF ausschließlich die Spendendaten „natürlicher Personen" mit dem vbPK SA ausgestattet werden sollen, ist das Bundesministeriums für Inneres diesfalls alleiniger Dienstleister der Stammzahlenregisterbehörde. Für die technische Realisierung der „Erstausstattung" wird es mehrere Varianten geben, die den unterschiedlichen technischen Ausstattungen der Zuwendungsempfänger entgegen kommen.

Näheres siehe Webseite des BMF:
(https://www.bmf.gv.at/steuern/selbstständige-unternehmer/einkommensteuer/FAQ-automatische-Datenuebermittlung-SA.html#heading_Wie_erfolgt_die_Ermittlung_des_verschluesselten_Personenkennzeichens_)

Die Schnittstellenbeschreibung „ § 18 EStG Sonderausgaben, technische Schnittstellenbeschreibung für den Austausch von Daten zum Zweck der bPK-Ausstattung" ist auf der BMF Webseite veröffentlicht:
(https://www.bmf.gv.at/top-themen/Technische_Schnittstellenbeschreibung.pdf?5qi4h6)

Ebenso sind die Antragsformulare für Spendenorganisationen zur Erstausstattung im Rahmen der technischen Variante „Online Anbindung" fertig gestellt. Erste Tests bezüglich einer Online-Anbindung wurden erfolgreich abgewickelt.

3.2.7 Amtswegige Prüfverfahren

Von 90 gemäß § 30 DSG 2000 amtswegig im Berichtszeitraum eingeleiteten Verfahren wurden 80 abgeschlossen.

Ausgewählte Verfahren:
Neben den amtswegigen Verfahren, die aufgrund anonymer Eingaben oder Eingaben durch Behörden erfolgen (bspw. zur Überprüfung der Rechtmäßigkeit einer Videoüberwachung), führt die Datenschutzbehörde jährlich Schwerpunktverfahren durch.

6 https://www.bmf.gv.at/steuern/BGBLA_2016_II_289.pdf?5s3q1c

Dabei wird ein bestimmter Sektor einer eingehenden datenschutzrechtlichen Überprüfung – einschließlich Vorortuntersuchungen – unterzogen.

2014/2015 wurden die wesentlichen Kreditauskunfteien näher geprüft. In den Jahren 2015/2016 wurden die größten Krankenanstaltenträger in allen neun Bundesländern einer Prüfung unterzogen.

a. D213.395 bis D213.399

Diese Verfahren dienten der Umsetzung des Prüfungsschwerpunktes 2015 im Krankenanstaltenbereich und wurden im Berichtszeitraum abgeschlossen. Die Datenschutzbehörde prüfte dabei bei insgesamt fünf öffentlichen Krankenanstaltenträgern in fünf Bundesländern, ob datenschutzrechtliche Bestimmungen eingehalten werden.

Das Prüfverfahren ergab, dass datenschutzrechtliche Bestimmungen im überwiegenden Ausmaß eingehalten werden und dass der Schutz personenbezogener Daten fester Bestandteil interner Beurteilungen und Verfahrensabläufe ist.

Dennoch wurden alle Verfahren mit Empfehlungen abgeschlossen, die im Rechtsinformationssystem des Bundes abrufbar sind.

Die Empfehlungen betreffen im Wesentlichen folgende Punkte:

- mangelnde Löschungsroutinen von Patientendaten sowie Daten ehemaliger Bediensteter
- mangelnde Kontrolle der Zugriffe auf Patientendaten
- überschießende Videoüberwachungen

b. D213.403

Dieses Prüfverfahren behandelte die Datenverwendung im Visa Informationssystem (VIS) durch das Bundesministerium für Inneres und das Bundesministerium für Europa, Integration und Äußeres. Die DSB ist aufgrund europarechtlicher Vorgaben verpflichtet, in regelmäßigen Abständen diese Datenverwendung zu prüfen. Das Verfahren wurde im Berichtszeitraum mit einer Empfehlung abgeschlossen, wonach ein neuer Dienstleistungsvertrag zwischen beiden Ministerien abgeschlossen werden möge und geeignete Maßnahmen ergriffen werden sollten, um eine effektive Zugriffskontrolle auf Daten in der VIS-Applikation sicherzustellen.

c. D213.468 bis D213.471

Diese Verfahren dienten der Fortsetzung der Umsetzung des Prüfungsschwerpunktes 2015/2016 im Krankenanstaltenbereich. Die Datenschutzbehörde prüfte dabei jene öffentlichen Krankenanstaltenträger in vier Bundesländern, die 2015 keiner Überprüfung unterzogen wurden. Diese Verfahren waren im Berichtszeitraum anhängig.

d. D213.475

Dieses Verfahren betrifft die Verwendung von Gesundheitsdaten in militärischen Sanitätszentren und ist vom Prüfungsschwerpunkt 2015/2016 umfasst. Im Berichtszeitraum war dieses Verfahren anhängig.

3.2.8 Äußerungen in Beschwerdeverfahren vor dem Bundesverwaltungsgericht

Die Datenschutzbehörde bearbeitete im Berichtszeitraum 35 neue Beschwerden an das Bundesverwaltungsgericht. Dies ist ein Anstieg gegenüber 2015, entspricht jedoch dem Anstieg der Bescheide zu Individualbeschwerden gemäß § 31 DSG 2000.

Es gab eine Beschwerde wegen Verletzung der Entscheidungspflicht, die aber vom Bundesverwaltungsgericht als unzulässig zurückgewiesen wurde.

Weitere Entscheidungen neben den hier angeführten können auf der Seite des Bundesverwaltungsgerichts im Rechtsinformationssystem des Bundes (RIS) nachgelesen werden.

Entscheidung W214 2106365-1 vom 11.01.2016

Der Beschwerdeführer hat nach einem Aufenthalt in einem Krankenhaus Mitarbeiter mit einer Flut an E-Mails konfrontiert, welche von den Betroffenen als aggressiv und bedrohlich empfunden wurde. Die Leitung des Krankenhauses informierte daher die Sicherheits¬behörden, schildete die Lage mündlich und übergab den Beamten ein E-Mail-Ausdrucke. Auf Frage der Sicherheitsbeamten wurden auch Informationen über den psychischen Gesundheitszustand des Beschwerdeführers mündlich weitergegeben. Dieser beschwerte sich bei der Datenschutzbehörde, die der Beschwerde „im Hauptpunkt" Folge gab und feststellte, dass die Leitung des Krankenhauses den Beschwerdeführer in seinem Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten verletzt habe indem sie Daten über dessen psychische Gesundheit an die Sicherheitsbehörden mündlich weitergegeben hatte.

Das Bundesverwaltungsgericht gab der Beschwerde des Krankenhauseses statt und entschied, dass eine Strafanzeige wegen Stalking (Beharrliche Verfolgung, § 107a Abs. 2 StGB) datenschutzrechtlich nicht überschießend ist, wenn der Beschwerdeführer Personen in einer Weise beharrlich verfolgt, die geeignet ist, sie in ihrer Lebensführung unzumutbar zu beeinträchtigen, indem er im Wege einer Telekommunikation oder unter Verwendung eines sonstigen Kommunikationsmittels oder über Dritte Kontakt zu ihr herstellt. Handlungen wie Auflauern, Nachstellen oder körperliche Übergriffe seien nicht erforderlich. Die Übermittlung der E-Mails sei zulässig gewesen, um den Sachverhalt zu untermauern. Die zusätzliche mündliche Übermittlung von Gesundheitsdaten sei zulässig, weil diese bereits in den E-Mails enthalten waren. Die mündliche Übermittlung einer zu Recht schriftlich übermittelten Information ist nicht unrechtmäßig, da diesbezüglich keine Geheimhaltungsinteressen verletzt werden können.

Entscheidung W101 2017257-1 vom 13.07.2016

Das Bundesverwaltungsgericht hat die Rechtsansicht der Datenschutzbehörde, dass für die Registrierung einer Videoüberwachungsanlage beim Datenverarbeitungs¬register eine Betriebsvereinbarung erforderlich sei, wenn die Anlage auch Daten von Mitarbeitern ermittelt, bestätigt. Eine Videoüberwachungsanlage diene zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personen¬bezogenen Daten der Arbeitnehmer im Sinne des § 96a Arbeitsverfassungsgesetz 1974 (ArbVG). Diese Datenermittlung geht zweifellos über die „Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen" hinaus. Auch wenn die gegenständliche Videoüberwachungsanlage nicht primär darauf abzielt, Mitar-

beiterdaten zu erfassen, so werden durch das eingesetzte Video-System dennoch (auch) Daten der Mitarbeiter - konkret Bilddaten - verarbeitet. Aus dem Wortlaut des § 96a Abs. 1 Z 1 ArbVG iVm § 50c Abs. 1 DSG 2000 ergebe sich daher die grundsätzliche Verpflichtung zum Abschluss einer Betriebsvereinbarung durch den Auftraggeber einer Videoüberwachungsanlage und deren Vorlage im Registrierungsverfahren (zumindest soweit beim Auftraggeber ein Betriebsrat eingerichtet ist).

3.2.9. Stellungnahmen zu Gesetzes- und Verordnungsvorhaben

Die DSB hat im Jahr 2016 zu folgenden Vorhaben eine Stellungnahme abgegeben. Die Stellungnahmen sind unter www.parlament.gv.at abrufbar.

- Abschlussprüfer-Aufsichtsgesetz (APAG)
- Jugendausbildungsgesetz
- Lohn- und Sozialdumping-Bekämpfungsgesetz;
- Arbeitsvertragsrechts-Anpassungsgesetz, Arbeitskräfteüberlassungsgesetz u.a., Änderung
- Bauarbeiter-Urlaubs- und Abfertigungsgesetz, Bauarbeiter-Schlechtwetterentschädigungsgesetz u.a., Änderung
- Schulrechtspaket 2016
- SFT-Vollzugsgesetz; Finanzmarktaufsichtsbehördengesetz, Investmentfondsgesetz 2011 u.a., Änderung
- Börsegesetz 1989, Änderung
- Präventions-Novelle 2016
- Gedenkstättengesetz
- Strafprozessordnung 1975, Staatsanwaltschaftsgesetz, Änderung
- Ärztegesetz, Änderung
- Sicherheitspolizeigesetz, Änderung
- Finanzmarkt-Geldwäschegesetz u.a
- Referenzwerte-Vollzugsgesetz
- Deregulierungsgesetz 2017 – Bundeskanzleramt
- Deregulierungsgesetz 2017 – Teil BMF/BMJ/BMFJ
- Gewerbeordnung, Änderung
- Innovationsstiftungsgesetz – ISG; Einkommensteuergesetz, Körperschaftsteuergesetz, Änderung
- Hochschülerinnen und Hochschülergesetz 2014
- Ingenieurgesetz 2017

4 Wesentliche höchstgerichtliche Entscheidungen

4.1 Verfassungsgerichtshof

Im Jahr 2016 hatte sich der Verfassungsgerichtshof (VfGH) nur am Rande mit datenschutzrechtlichen Fragen zu befassen. Insbesondere wurde über kein verwaltungsgerichtliches Erkenntnis inhaltlich entschieden, das einen Bescheid der Datenschutzbehörde zum Gegenstand hatte.

Im Beschluss vom 25.2.2016, E 2424/2015, wurde die inhaltliche Behandlung der Beschwerde gegen das Erkenntnis des Bundesverwaltungsgerichts vom 20.10.2015, GZ: W224 2113499-1/4E, durch das der Bescheid der Datenschutzbehörde vom 11.8.2015, GZ: DSB-D122.359/0005-DSB/2015 (Zulässigkeit der Veröffentlichung von EU-Agrarförderungsdaten), bestätigt worden war, mit kurzer Begründung abgelehnt.

Im Beschluss vom 13.10.2016, G 330/2015, hat der VfGH einen Individualantrag auf Aufhebung datenschutzrechtlich relevanter Bestimmungen des Gesundheitstelematikgesetzes u.a. mangels ausreichender Darlegung der Betroffenenrolle und damit der Antragslegitimation des den Antrag stellenden Arztes zurückgewiesen, ohne auf datenschutzrechtliche Fragen näher einzugehen.

Ähnliches gilt für den Beschluss vom 24.11.2016, V 24/2016, in dem ein Individualantrag eines flugmedizinischen Sachverständigen auf Aufhebung einer Verordnung der Austro Control Ges.m.b.H. betreffend die Verwendung des Datenübertragungssystems EMPIC wegen bereits erfolgten Außerkrafttretens der angefochtenen Rechtsvorschrift zurückgewiesen wurde.

4.2. Oberster Gerichtshof

4.2.1 OGH in Strafsachen in 15 Os176/15v vom 13.01.2016

Durch § 7 MedienG geschützt wird der höchstpersönliche Lebensbereich als Kernbereich des durch Art 8 MRK gewährten Anspruchs auf Achtung des Privat- und Familienlebens. Jede (zulässige) Verfügung über eine solche Rechtsposition - wie etwa die Zustimmung im Sinn des § 7 MedienG - stellt ebenfalls die Ausübung eines höchstpersönlichen Rechts dar. Für diese gilt ganz allgemein der Grundsatz, dass sie mit einer gesetzlichen Vertretung unvereinbar sind. Für ihre Ausübung ist vielmehr die natürliche Einsichts- und Urteilsfähigkeit erforderlich. Fehlt diese Einsicht, so kann ein höchstpersönliches Recht weder durch gesetzliche Vertreter oder Sachwalter noch durch das Pflegschaftsgericht ersetzt werden (6 Ob 106/03m).

Mit Beschluss vom 13.01.2016 zu Zl. 15 Os 176/15v[7] hat der Oberste Gerichtshof einen Erneuerungsantrag gegen das Urteil des Oberlandesgerichtes Wien (AZ 18 Bs 63 / 15 v) gemäß § 363b Abs. 2 Z3 als offenbar unbegründet zurückgewiesen.

7 RIS Link: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20160113_OGH0002_0150OS00176_15V0000_000&ResultFunctionToken=333e9ace-4bc8-4e76-8383-4ebd90002dc0&Position=1&Gericht=&Rechtssatznummer=&Rechtssatz=&Fundstelle=&AenderungenSeit=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=15+Os+176%2F15v&VonDatum=&BisDatum=

Im zu Grunde liegenden Fall hatte das Medium über den Sturz eines 10-jährigen Mädchens aus dem Fenster eines Kinderheims berichtet, wobei dem Artikel ein lediglich leicht verpixeltes Lichtbild des Mädchens beigefügt war. Die Mutter des mj. Kindes hatte einer Mitarbeiterin der Medieninhaberin ein Interview gegeben und auch das Lichtbild des Mädchens übermittelt.

Gegen das Urteil des Landesgerichtes Wien richtete sich der Erneuerungsantrag des Medieninhabers, der eine Verletzung des Art 10 MRK (Freiheit der Meinungsäußerung) darin erblickte, dass das Oberlandesgericht Wien den Ausschlussgrund nach § 7 Abs 2 Z 3 MedienG (Bem.: dass nach den Umständen angenommen werden konnte, dass der Betroffene mit der Veröffentlichung einverstanden war) nicht angenommen hatte.

Der OGH kam im gegenständlichen Fall zum Schluss, dass die fehlende Einwilligung des mj. Mädchens nicht durch eine Willenserklärung der Kindesmutter substituiert werden kann.

Der OGH hielt aber auch fest, dass die Rechtsdurchsetzung selbst nämlich nicht „vertretungsfeindlich" ist, sie kann nach Rechtsverletzungen an (hier:) Unmündigen durch deren gesetzliche Vertreter erfolgen, auch wenn es um ein Persönlichkeitsrecht geht.

4.2.2 OGH in 6 Ob 26/16s, 30.03.2016, Privat gg. Google Inc.

„Keine Untersagung der Namensergänzung durch Google Auto – Vervollständigung wenn bei Eingabe des ursprünglichen Namens auch eine Namensänderung nach § 2 Abs. 1 Z 11 Namensänderungsgesetz („Namensänderung aus sonstigen Gründen") angezeigt wird. Aber: Haftung des Suchmaschinenbetreibers", wenn er trotz Hinweises durch einen Betroffenen einen die Persönlichkeitsrechte verletzenden Ergänzungsvorschlag der Auto-Vervollständigungsfunktion nicht beseitigt".

Mit Beschluss vom 30.03.2016 zu Zl. in 6 Ob 26/16s[8] hat der Oberste Gerichtshof den Revisionsrekurs einer Klägerin im Rahmen eines Provisorialbegehrens auf Unterlassung der automatischen Vervollständigung des Suchbegriffs ihres Geburtsnamen/ursprünglichen Namens um den – gemäß § 2 Abs. 1 Z. 11 Namensänderungsgesetz - abgeänderten Namen („Namensänderung aus sonstigen Gründen") abgewiesen.

Hintergrund:
Die Klägerin war mit ihrem ursprünglichen Namen in den Niederlanden als Zahnärztin eingetragen. Sie erhielt erstmals im Mai 2007 und im April 2008 einen Verweis von der Niederländischen Standesaufsichtsbehörde. Auf eigenen Wunsch wurde die Klägerin Anfang 2008 von der niederländischen Liste der Zahnärzte gestrichen. Mit 28.4.2008 wurde mit Bescheid der Stadt Innsbruck eine Namensänderung gemäß § 2 Abs. 1 Z 11 NÄG („aus sonstigen Gründen") bewilligt. Der Klägerin gelang es daraufhin (mit dem neuen Namen) in die britische Liste der Zahnärzte aufgenommen zu werden (zuvor war dem Antrag mit ihrem ursprünglichen Namen nicht entsprochen worden).

4.2.3 OGH in 7 Ob 81/16m, 06.07.2016, Besuchskontaktfotos im Internet

Untersagung Lichtbilder und persönliche Daten eines Minderjährigen einem nicht zur Familie gehörenden Dritten zur Einstellung in die Website „*****" und vergleichbare Internet-Portale oder in vergleichbarer Weise zugänglich zu machen, sofern die obsorgeberechtigte Mutter hiezu nicht ihre ausdrückliche Einwilligung erteilt.

8 02.02.2016&Norm=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=
RIS Link: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=
JJT_20160330_OGH0002_0060OB00026_16S0000_000

Mit Beschluss vom 06.07.2016 zu Zl. 7 Ob 81/16m[9] hat der Oberste Gerichtshof einem Revisionsrekurs im Rahmen eines Provisorialbegehrens auf Untersagung teilweise Folge gegeben, nämlich „Lichtbilder und persönliche Daten eines Minderjährigen einem nicht zur Familie gehörenden Dritten zur Einstellung in die Website „*****“ und vergleichbare Internet-Portale oder in vergleichbarer Weise zugänglich zu machen, sofern die obsorgeberechtigte Mutter hiezu nicht ihre ausdrückliche Einwilligung erteilt hat. Das Mehrbegehren auf Löschung der Lichtbilder auf den Internetseiten wurde abgewiesen, da eine Verfügungsberechtigung des Antragsgegners betreffend das inkriminierte Lichtbild und die Daten auf der Homepage seiner Vertrauensperson nicht bescheinigt war und die Internetseite auch nicht vom Antragsgegner betrieben wurde.

Der OGH stellte dazu fest, dass im vorliegenden Fall der Antragsgegner das den Antragsteller zeigende Lichtbild angefertigt und weitergegeben hat und dieses letztlich in den Verfügungsbereich der Vertrauensperson des Antragsgegners gelangte und von diesem im Internet auf dessen Homepage veröffentlicht wurde.

4.3 Verwaltungsgerichtshof

4.3.1 VwGH, Ra 2016/04/0044 vom 23. November 2016

Beim Recht auf Auskunft nach § 26 DSG 2000 handelt es sich um ein höchstpersönliches und somit um ein nicht übertragbares Recht. Das bedeutet, dass in das Recht auf Auskunft keine Rechtsnachfolge stattfindet und es mit dem Tod der betroffenen Person erlischt.

In dieser Entscheidung des Verwaltungsgerichtshofes (VwGH) ging es um die Frage, ob es sich beim datenschutzrechtlichen Auskunftsrecht (§ 26 DSG 2000) um ein höchstpersönliches Recht handelt, das nur vom Betroffenen selbst geltend gemacht werden kann.

Im konkreten Fall war dem Masseverwalter über das Vermögen eines verstorbenen Rechtsanwalts eine datenschutzrechtliche Auskunft im Zusammenhang mit dessen Bonität verweigert worden. Der Masseverwalter hatte sich in der Folge dagegen erfolglos an die Datenschutzbehörde und an das Bundesverwaltungsgericht gewendet.

Der VwGH führte unter Hinweis auf die Gesetzesmaterialien und die Rechtsprechung der anderen Höchstgerichte aus, dass es sich beim Auskunftsrecht um ein höchstpersönliches Recht handelt. Als solches kann es vom Masseverwalter nicht geltend gemacht werden. Des Weiteren führte der VwGH aus, dass das Recht auf Auskunft – wie auch das Recht auf Löschung – trotz seiner möglicherweise vermögensrechtlichen Konsequenzen nicht als vermögensrechtliches Recht einzustufen ist. Die Revision wies der VwGH daher als unbegründet ab.

4.3.2 VwGH, Ro 2015/04/0011 vom 12. September 2016

Eine „Dashcam“ (Kamera im Auto zur Beweissicherung) mit „SOS-Button“ (Notfallknopf), die beim Auslösen des Notfallknopfs beliebig und dauerhaft Geschehnisse außerhalb des Autos aufzeichnet, ist unzulässig.

9 RIS: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20160706_OGH0002_0070OB00081_16M0000_000&ResultFunctionToken=5645cb24-e894-4732-90fe-be24db11b89c&Position=1&Gericht=&Rechtssatznummer=&Rechtssatz=&Fundstelle=&AenderungenSeit=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=7Ob81/16m&VonDatum=&8isDatum=20.07.2016&Norm=&lmRisSeit=Undefined&ResultPageSize=100&Suchworte=

In dieser Entscheidung des Verwaltungsgerichtshofes (VwGH) ging es um die Frage, ob der Einsatz einer „Dashcam" mit beliebig zu aktivierendem Notfallknopf zulässig ist.

In seinem - vor dem VwGH angefochtenen - Erkenntnis argumentierte das Bundesverwaltungsgericht (BVwG) , dass der Einsatz von „Dashcams" deshalb unzulässig sei, weil es einem Privaten, der eine „Dashcam" benütze, prinzipiell an der Befugnis zur Überwachung des öffentlichen Raums mangle.

Der VwGH bestätigt die Entscheidung, verwirft allerdings diese Begründung und kommt über eine Verhältnismäßigkeitsprüfung zum selben Ergebnis. Er führt dazu aus, dass das konkrete verfahrensgegenständliche Modell der Dashcam unzulässig ist, da die dauerhafte Speicherung von Bilddaten durch das Auslösen eines sogenannten „SOS-Button" erfolgt und dieser jederzeit - somit ohne Einschränkungen - betätigt werden kann. Aus diesem Grund ist es nach Ansicht des VwGH ausgeschlossen, das vorliegende System als gelindestes Mittel im Sinn des § 7 Abs. 3 DSG 2000 anzusehen. § 7 Abs. 3 DSG 2000 sieht nämlich vor, dass Eingriffe in das Grundrecht auf Datenschutz (hier: von jenen Personen, die von der „Dashcam" aufgezeichnet werden), nur im erforderlichen Maß und mit den gelindesten Mitteln erfolgen dürfen.

4.3.3 VwGH, Ra 2016/04/0014 vom 4. Juli 2016

Ein datenschutzrechtlicher Auftraggeber hat jeder Person, die ihre Identität in geeigneter Form nachweist, Auskunft über die zu dieser Person verarbeiteten Daten zu geben. Eine Meldebestätigung nach § 19 MeldeG stellt keinen solchen geeigneten Identitätsnachweis dar.

Nach dem Datenschutzgesetz 2000 hat ein datenschutzrechtlicher Auftraggeber grundsätzlich jeder Person Auskunft über die zu ihr verarbeiteten Daten zu erteilen; dies allerdings nur unter der Voraussetzung, dass die auskunftswerbende Person ihre Identität „in geeigneter Form" nachweist.

In dieser Entscheidung beschäftigte sich der Verwaltungsgerichtshof (VwGH) näher mit den Anforderungen an einen solchen geeigneten Identitätsnachweis.

Er traf eine Kernaussage dahingehend, dass die Vorlage eines Identitätsdokuments in Form einer öffentlichen Urkunde jedenfalls als Nachweis ausreicht. Eine Meldebestätigung nach § 19 Meldegesetz stellt hingegen keinen solchen Identitätsnachweis dar.

Schreitet ein Rechtsanwalt für die auskunftswerbende Person ein, ist kein weiterer Identitätsnachweis erforderlich. Vor Gerichten oder Behörden genügt in diesem Fall die Berufung auf die anwaltliche Vollmacht. Gegenüber Auftraggebern des privaten Bereichs reicht die Berufung auf die anwaltliche Bevollmächtigung hingegen nicht aus. Der Auftraggeber kann hier zusätzlich den urkundlichen Nachweises der Bevollmächtigung verlangen.

Ein Identitätsnachweis muss nicht in jedem Fall formstreng erbracht werden. Es kann ausreichend sein, wenn Anhaltspunkte dafür bestehen, dass der Auftraggeber keine Zweifel an der Identität der auskunftswerbenden Person haben musste.

4.4 Europäischer Gerichtshof

4.4.1 C-203/15 und C-698/15 – Urteil des EuGH vom 21.12.2016 – Vorratsdatenspeicherung

Der EuGH hatte sich in der gegenständlichen Rechtssache mit der Frage zu beschäftigen, ob, und wenn ja, welche Auswirkungen seine Entscheidung zur Aufhebung der Richtlinie zur Vorratsdatenspeicherung (Digital Rights Ireland u. a. (C-293/12 und C-594/12)) auf nationale Regelungen über eine Vorratsdatenspeicherung haben.

Im Urteil verwies der EuGH zunächst darauf, dass eine nationale Regelung über eine allgemeine und unterschiedslose Vorratsdatenspeicherung für Zwecke der Bekämpfung von Straftaten nicht zulässig ist. Der EuGH hielt jedoch ausdrücklich fest, dass eine Vorratsdatenspeicherung für Zwecke der Bekämpfung schwerer Kriminalität unter Beachtung gewisser Kriterien zulässig sein kann.

Der EuGH präzisierte, dass eine nationale Regelung über eine Vorratsdatenspeicherung klare und präzise Regeln vorsehen sowie Mindesterfordernisse aufstellen muss, damit jene Personen, deren Daten auf Vorrat gespeichert werden, über einen wirksamen Schutz ihrer personenbezogenen Daten verfügen. Eine nationale Regelung muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen (Einschränkung des Zeitraums, eines geografischen Gebietes und/oder eines Personenkreises) Daten auf Vorrat gespeichert werden dürfen, um zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird.

Eine nationale Regelung muss weiters auch materiell- und verfahrensrechtliche Voraussetzungen über den Zugang der zuständigen nationalen Behörden zu den Daten festlegen und hat der Zugang grundsätzlich – außer in hinreichend begründeten Einzelfällen – einer vorherigen Kontrolle durch ein Gericht oder einer unabhängigen Verwaltungsstelle zu unterliegen. Darüber hinaus müssen betroffene Personen über einen allfälligen Zugriff auf ihre Daten in Kenntnis gesetzt werden und müssen Vorratsdaten im Unionsgebiet gespeichert und nach Ablauf ihrer Speicherfrist vernichtet werden.

4.4.2 Urteil in der Rs C-582/14 dynamische IP Adressen

SV: öffentliche Einrichtungen in D stellen Informationen auf Internetportalen bereit; Zugriffe auf diese werden protokolliert (deswegen -> Klage auf Unterlassung). Im Verfahren der Vorinstanz stellte sich die Frage inwiefern dynamische IP-Adressen personenbezogene Daten sind – diese sind ohne weitere Daten, über welche nur Dritte verfügen nicht auf die Nutzer zurückzuführen.

D wurde verurteilt die Speicherung über das Ende der Nutzungsdauer hinaus zu unterlassen.

Vorlagefrage: 1. Art. 2 Buchst. a der RL 95/46/EG ist eine IP-Adresse schon dann ein personenbezogenes Datum wenn das Zusatzwissen für die Rückführbarkeit Dritte haben.

2. Verbietet Art. 7 Buchst. F leg. cit. eine nationale Regelung mit dem Inhalt, dass die Daten von Nutzern nur mit dessen Einwilligung oder nur soweit sie zur Anwendernutzung und Abrechnung erforderlich sind erhoben und verwendet werden dürfen und die generelle Funktion der Anwendung keine Datenspeicherung über den Nutzervorgang hinaus rechtfertigen würde.

Schlussantrag GA: ad 1) der GA ist der Meinung, dass dies zu bejahen ist, weil nicht nur die hypothetische Möglichkeit besteht, dass sich der Diensteanbieter die Daten von dem bestimmbaren Dritten verschaffen kann und damit die IP-Adresse in ein personenbezogenes Faktum verwandelt.

Ad 2) Die deutsche Verwaltung ist in diesem Falle als nicht hoheitlich anzusehen. § 15 TMG ist restriktiver als das Unionsrecht weil kein anderes als Interesse der Abrechnung vorgesehen ist; deshalb ist es nicht im Rahmen von Art. 5 RL 95/46 (keine Konkretisierung sondern Einschränkung)

Vorschlag das GA: 1) Gemäß Art. 2 Buchst. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist eine dynamische IP-Adresse, über die ein Nutzer die Internetseite eines Telemedienanbieters aufgerufen hat, für Letzteren ein „personenbezogenes Datum", soweit ein Internetzugangsanbieter über weitere zusätzlichen Daten verfügt, die in Verbindung mit der dynamischen IP-Adresse die Identifizierung des Nutzers ermöglichen.

2) Art. 7 Buchst. f der Richtlinie 95/46 ist dahin auszulegen, dass der Zweck, die Funktionsfähigkeit des Telemediums zu gewährleisten, grundsätzlich als ein berechtigtes Interesse anzusehen ist, dessen Verwirklichung die Verarbeitung dieses personenbezogenen Datums rechtfertigt, sofern ihm Vorrang gegenüber dem Interesse oder den Grundrechten der betroffenen Person zuerkannt worden ist. Eine nationale Rechtsvorschrift, die die Berücksichtigung dieses berechtigten Interesses nicht zulässt, ist mit dem genannten Artikel nicht vereinbar.

4.4.3 C .191/15 VKI gegen Amazon EU Sàrl

Bei Amazon EU Sàrl handelt es sich um eine internationale Versandhandelsgruppe, die ihren Sitz in Luxemburg hat. Diese Gesellschaft, welche in Österreich weder Sitz noch Niederlassung hat, wendet sich im Rahmen ihrer Geschäftstätigkeit mit der Top-Level-Domain „.de" an Verbraucher mit Wohnsitz in Österreich. Im Ausgangsverfahren erhob der Verein für Konsumenteninformation (VKI) eine Unterlassungsklage gegen Amazon EU woraufhin der Fall in weiterer Folge dem EuGH zur Vorabentscheidung vorgelegt wurde. Dabei stellte sich die Frage, ob die Verarbeitung personenbezogener Daten durch ein Unternehmen, das im elektronischen Geschäftsverkehr mit Verbrauchern, die in anderen Mitgliedstaaten ansässig sind, Verträge abschließt, nach Art. 4 Abs. 1 lit. a der Richtlinie 95/46/EG unabhängig vom sonst anwendbaren Recht ausschließlich dem Recht jenes Mitgliedstaats, in dem sich die Niederlassung des Unternehmens befindet, in deren Rahmen die Verarbeitung stattfindet, unterliegt oder ob das Unternehmen auch die Datenschutzvorschriften jener Mitgliedstaaten zu beachten hat, auf die es seine Geschäftstätigkeit ausrichtet.

Der EuGH führte in seinem Urteil aus, der Begriff der Niederlassung stellt auf jede tatsächliche und effektive Tätigkeit, die mittels einer festen Einrichtung ausgeübt wird ab – selbst wenn sie nur geringfügig ist. Eine Niederlassung kann nicht bloß deswegen bestehen, weil von dort aus auf die Website des fraglichen Unternehmens zugegriffen werden kann. Vielmehr sind sowohl der Grad an Beständigkeit der Einrichtung als auch die effektive Ausübung der wirtschaftlichen Tätigkeiten im fraglichen Mitgliedstaat zu bewerten (vgl. Urteil Weltimmo, C-230/14). Die in Rede stehende Verarbeitung personenbezogener Daten muss dabei nicht von der betreffenden Niederlassung selbst ausgeführt werden, sondern lediglich „im Rahmen der Tätigkeiten" der Niederlassung stattfinden. Es ist dabei Sache des vorlegenden Gerichts, im Licht dieser Rechtsprechung und unter Berücksichtigung aller relevanten Umstände des Ausgangsverfahrens zu bestimmen, ob Amazon EU die fragliche Verarbeitung personenbezogener Daten im Rahmen

der Tätigkeiten einer Niederlassung vornimmt, die sich in einem anderen Mitgliedstaat als Luxemburg befindet. Sollte das vorlegende Gericht feststellen, dass sich die Niederlassung, in deren Rahmen Amazon EU die Verarbeitung dieser Daten vornimmt, in Deutschland befindet, unterläge diese Verarbeitung deutschem Recht.

Art. 4 Abs. 1 lit. a der Richtlinie 95/46/EG ist demnach dahingehend auszulegen, dass eine Verarbeitung personenbezogener Daten durch ein im elektronischen Geschäftsverkehr tätiges Unternehmen dem Recht jenes Mitgliedstaats unterliegt, auf den das Unternehmen seine Geschäftstätigkeit ausrichtet, wenn sich zeigt, dass das Unternehmen die fragliche Datenverarbeitung im Rahmen der Tätigkeiten einer Niederlassung vornimmt, die sich in diesem Mitgliedstaat befindet. Es ist Sache des nationalen Gerichts, zu beurteilen, ob dies der Fall ist.

5. Datenschutz-Grundverordnung und Vorbereitungsmaßnahmen der DSB zur Anwendung ab 25. Mai 2018

Nach der politischen Einigung im Dezember 2015 wurde die Datenschutz-Grundverordnung (DSGVO) am 4. Mai 2016 als „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ im Amtsblatt Nr. L 119 S. 1 veröffentlicht.

Sie trat am zwanzigsten Tag nach ihrer Veröffentlichung in Kraft und gilt ab dem 25. Mai 2018.

Zeitgleich wurde die Richtlinie (EU) des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates – Datenschutz-Richtlinie Polizei Justiz (DSRL-PJ) im Amtsblatt Nr. L 119 S. 89 kundgemacht.

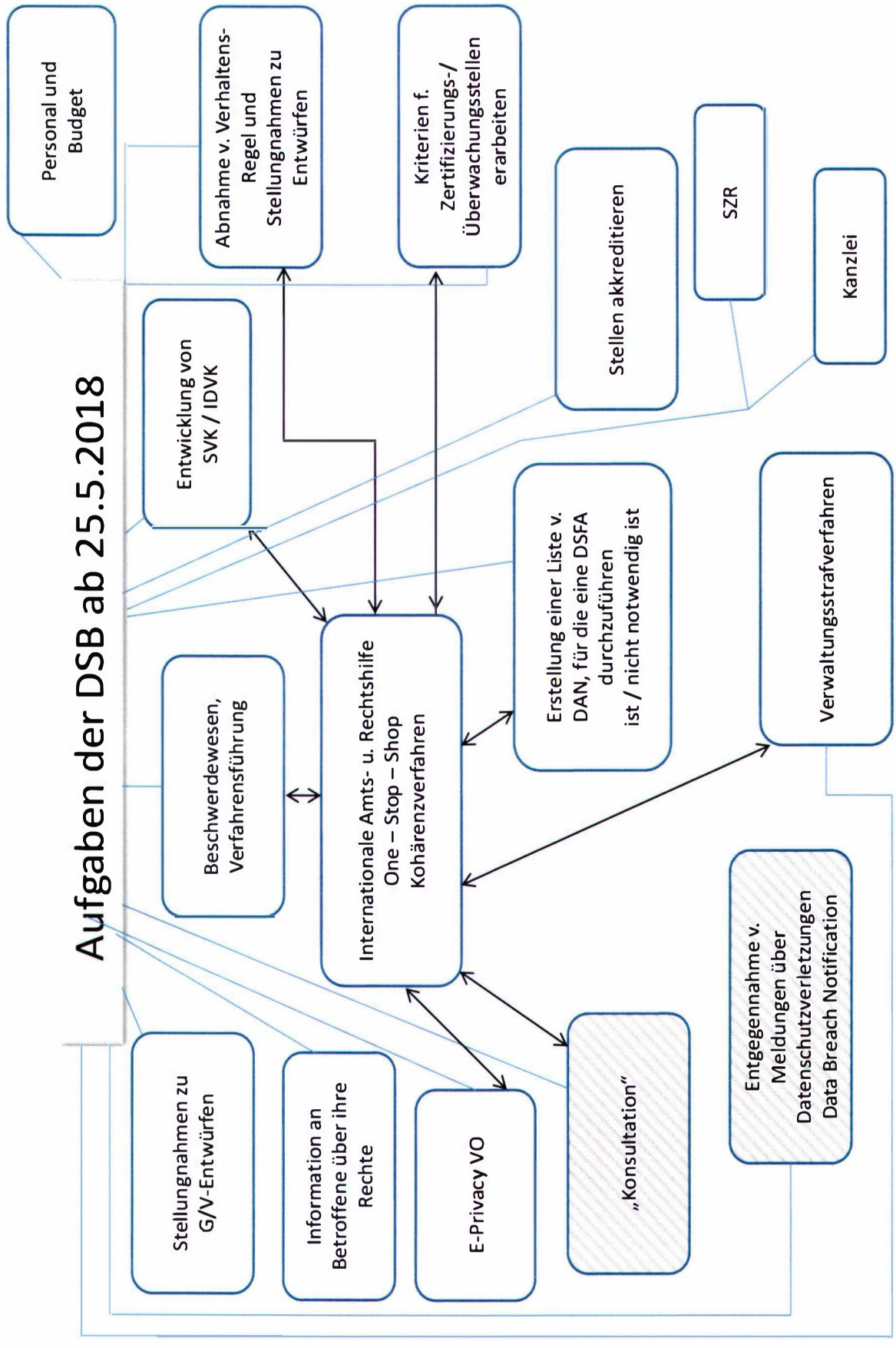
Das Jahr 2016 war daher intensiven behördeninternen Vorbereitungen auf den neuen europaweiten Rechtsrahmen gewidmet.

Soweit es die Aufgaben und Befugnisse der Aufsichtsbehörde nach der DSGVO betrifft, sind diese im Wesentlichen in Art. 57 und 58 DSGVO normiert und lassen sich graphisch wie folgt zusammenfassen:

Die weiß hinterlegten Felder weisen jene Aufgaben aus, die die DSB bereits derzeit wahrnimmt.

Die grau schraffierten Felder stellen jene Aufgaben dar, die zwar in ihrem Umfang neu sind, jedoch Anknüpfungspunkte zu bereits bekannten Verfahrenstypen aufweisen (bspw. DVR-Verfahren, Verfahren nach § 95a TKG 2003).

Die grau hinterlegten Felder sind gänzlich neue Aufgaben.


Aufgaben der DSB ab 25.5.2018
Personal und Budget
Abnahme v. Verhaltens-Regel und Stellungnahmen zu Entwürfen
Kriterien f. Zertifizierungs-/ Überwachungsstellen erarbeiten
Stellen akkreditieren
SZR
Kanzlei
Entwicklung von SVK / IDVK
Beschwerdewesen, Verfahrensführung
Internationale Amts- u. Rechtshilfe One – Stop – Shop Kohärenzverfahren
Erstellung einer Liste v. DAN, für die eine DSFA durchzuführen ist / nicht notwendig ist
Verwaltungsstrafverfahren
Stellungnahmen zu G/V-Entwürfen
Information an Betroffene über ihre Rechte
E-Privacy VO
„Konsultation"
Entgegennahme v. Meldungen über Datenschutzverletzungen Data Breach Notification

Die Datenschutzbehörde hat daher zur Sicherstellung einer reibungslosen Umsetzung folgende interne Maßnahmen im Berichtszeitraum ergriffen:

- interne Schulungen der Bediensteten
- regelmäßige Beiträge im Newsletter zur DSGVO und auf der Website der DSB
- genaue Analyse der einzelnen Kapitel der DSGVO durch bestimmte Bedienstete mit regelmäßigen Präsentationen im Rahmen interner Besprechungen
- verstärkte Teilnahme an maßgeblichen Untergruppen der Art. 29-Gruppe (Cooperation Subgroup, Future of Privacy Subgroup, International Transfer Subgroup, Key Provisions Subgroup etc.) zur Vorbereitung von Guidelines und der Zusammenarbeit der Behörden
- Informations- und Vernetzungstreffen für Behörden und öffentliche Stellen im Oktober 2016
- regelmäßiger Kontakt zu Plattformen behördlicher und betrieblicher Datenschutzbeauftragter
- Ausarbeitung eines Planspiels eines grenzüberschreitenden Sachverhaltes; dieses Planspiel soll 2017 mit einer Partnerbehörde durchgeführt werden, um die Verfahrensabläufe bei grenzüberschreitenden Verfahren zu erproben und zu optimieren
- Teilnahme der Mitarbeiterinnen und Mitarbeiter der DSB an Sitzungen und Konferenzen, die der DSGVO gewidmet sind (in unterschiedlichen Rollen)

Darüber hinaus waren und sind Vertreter und Vertreterinnen der Datenschutzbehörde regelmäßig als Referenten zu Vorträgen zur DSGVO eingeladen. Weiters veröffentlichten Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörde Beiträge zur DSGVO in einschlägigen Druckwerken.

6. Europäische Zusammenarbeit

6.1 Europäische Union

6.1.1 Die Art. 29 Datenschutzgruppe

Diese nach Art. 29 der Datenschutz-Richtlinie benannte Gruppe ist das Forum sämtlicher Datenschutzbehörden des EWR.

Sie tagt sechsmal pro Jahr im Plenum, wobei an diesen Sitzungen im Regelfall die jeweiligen BehördenleiterInnen sowie der Europäische Datenschutzbeauftragte teilnehmen und Vertreter der Europäischen Kommission teilnehmen.

Zur Vorbereitung dieser Sitzungen sowie zur Vorbereitung von zu beschließenden Dokumenten sind diverse Untergruppen eingerichtet, die sich mit sektorspezifischen Fragen des Datenschutzes auseinandersetzen.

Im Hinblick auf die Umsetzung der DSGVO sowie das Inkrafttreten des neuen Angemessenheitsbeschlusses der Europäischen Kommission betreffend die USA (Privacy Shield; Durchführungsbeschluss (EU) 2016/1250) haben Bedienstete der DSB im Jahr 2016 vorrangig an jenen

Untergruppen der Art. 29-Gruppe teilgenommen, die den Übergang auf den neuen Rechtsrahmen vorbereiten und der Umsetzung des Privacy Shield gewidmet sind.

Dazu wurden von der Art. 29-Gruppe bereits folgende Leitlinien vorbereitet, die auf der Website der Europäischen Kommission (vorerst nur in englischer Sprache) abrufbar sind:

- Guidelines on the right to data portability
- Guidelines on Data Protection Officers
- Guidelines for identifying a controller or processor's lead supervisory authority

Bei den von der DSB beschickten Untergruppen der Art. 29-Gruppe handelt es sich um

a. die Cooperation Subgroup

b. die Key Provisions Subgroup

c. die Future of Privacy Subgroup

d. die Technology Subgroup

e. die International Transfer Subgroup

f. die Financial Matters Subgroup

g. die Border, Travel and Law Enforcement Subgroup (BTLE)

Daneben leitet und koordiniert die Datenschutzbehörde die E-Government-Subgroup.

Zu den einzelnen Untergruppen im Detail.

a. Cooperation Subgroup
Diese Untergruppe dient der Vorbereitung auf die in Kapitel VII DSGVO vorgesehene grenzüberschreitende Kooperation zwischen den Aufsichtsbehörden sowie der Vorbereitungen auf den Europäischen Datenschutz-Ausschuss, der die Art. 29-Gruppe ablösen wird.

b. Key Provisions Subgroup
Diese Untergruppe befasst sich, unvorgreiflich einer rechtsverbindlichen Auslegung durch den EuGH, mit ausgewählten Begriffen der DSGVO und deren Interpretation. Diese Untergruppe hat zwei am 13. Dezember 2016 vom Plenum beschlossene Leitlinien (Guidelines on Data Protection Officers, Guidelines for identifying a controller or processor's lead supervisory authority) vorbereitet, die die Bestimmungen der DSGVO betreffend Datenschutzbeauftragte (Art 37 bis 29 DSGVO) und die Bestimmung der federführenden Aufsichtsbehörde (Art 56 DSGVO) erläutern, um insbesondere künftigen Verantwortlichen Hilfestellung bei der Erfüllung ihrer Pflichten zu geben.

c. Future of Privacy Subgroup
Diese Untergruppe, in der vorrangig die jeweiligen Behördenleiter vertreten sind, bereitet strittige Fragen für das Plenum der Art. 29-Gruppe auf und dient zudem der Klärung grundsätzlicher Fragen zu Entwicklungen im Datenschutzrecht.

d. Technology Subgroup
Diese Untergruppe befasst sich mit Technologien und deren Auswirkungen auf den Datenschutz, ua. Drohnen oder Cookie-Technologie. Die Untergruppe hat im Berichtszeitraum den Übergang zur Datenschutz-Grundverordnung vorbereitet ua. zum Recht auf Datenübertragbarkeit (Art. 20 DSGVO) und zur Datenschutz-Folgenabschätzung (Art. 35 DSGVO).

e. International Transfer Subgroup
Diese Untergruppe beschäftigt sich mit Themen rund um Datenübertragungen von der EU in Drittstaaten. Ein besonderes Augenmerk liegt dabei auf der Befassung mit Fragen, Maßnahmen, Regelungen etc. betreffend den EU-US-Datenschutzschild (EU-US Privacy Shield).

f. Financial Matters Subgroup
Diese Untergruppe befasst sich mit datenschutzrechtlichen Fragen im Bereich des Zoll-, Bank- und Steuerwesens.

g. BTLE
Die Borders Travel & Law Enforcement Untergruppe beschäftigt sich beispielsweise mit Fragen der Umsetzung der Datenschutz-Richtlinie für Polizei und Strafjustiz (Richtlinie (EU) 2016/680) sowie mit der Umsetzung der Richtlinie über die Verwendung von Fluggastdatensätzen (Passenger Name Record-Daten; Richtlinie (EU) 2016/681). Auch beschäftigt sich die Untergruppe mit den datenschutzrechtlichen Aspekten von unionsrechtlichen Normvorschlägen zu IT-Systemen für Grenzübertritte („Stronger and Smarter Information Systems for Borders and Security").

h. E-Government Subgroup
Die e-Government Gruppe hat sich 2016 mit folgenden Themen beschäftigt:
Veröffentlichungen personenbezogener Daten zu Transparenzzwecken.
2 Verhaltensregeln im Sinne von Art 27 der Richtlinie 95/46/EG wurden begutachtet.
Umfang und Arten des Einsatzes von Cloud Diensten durch Auftraggeber des öffentlichen Bereichs wurde erhoben und diskutiert.

6.1.2 Europol

Europol ist eine europäische Polizeibehörde mit der Aufgabe die Leistungsfähigkeit der zuständigen Behörden der Mitgliedstaaten und ihre Zusammenarbeit zu verbessern im Hinblick auf die Verhütung und die Bekämpfung des Terrorismus, des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität. Europol verarbeitet zu diesem Zweck große Mengen von vor allem strafrechtsrelevanten Daten. Diese Verarbeitung unterliegt bis Mai 2017 der besonderen Kontrolle durch eine gemeinsame Kontrollinstanz, die aus Vertretern aller EU Datenschutzbehörden besteht, dem „Europol Joint Supervisory Body" (JSB) der auf Grundlage des Art. 34 des Europol Beschlusses[10] eingerichtet wurde. Mit der Europol Verordnung[11] 794/2016 vom 11. Mai 2016, die am 1.Mai 2017 in Kraft tritt, wird diese gemeinsame Kontrollinstanz ersetzt. An Ihre Stelle tritt eine geteilte Kontrolle. Einerseits durch nationale Kontrollinstanzen, die die Zulässigkeit der Eingabe und des Abrufs personenbezogener Daten sowie jedweder Übermittlung dieser Daten an Europol überwachen und andererseits den europäischen Datenschutzbeauftragten (EDPS), der die Verarbeitung durch Europol überwacht.

10 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:de:PDF
11 http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0794&from=EN

Überprüft wurden im Berichtsjahr von der gemeinsamen Kontrollinstanz im Zuge der jährlichen Inspektion a. die Verwendung und Auswertung der vorhandenen Datensammlungen (vor allem analytische Auswertungen zur Verbrechensbekämpfung), b. die im Europol Informationssystem (Fahndungssystem) gespeicherten Daten sowie c. die in der Personalverwaltung von Europol eingesetzten Datenanwendungen.

Neben dieser regelmäßigen Prüfungstätigkeit hat die gemeinsame Kontrollinstanz beschlossen, eine vertiefte Prüfung der Internet-Recherchen und Auswertungen von Europol vorzunehmen und die Erstellung einer Webseite mit Fahndungsausschreibungen aus allen EU Mitgliedsstaaten (EU most wanted list) untersucht. Zu den Zusammenarbeitsübereinkommen zwischen Europol und Georgien[12] bzw. der Ukraine [13] wurden positive Stellungnahmen abgegeben.

6.1.3 Schengen

Das Schengener Informationssystem, das gemäß den Bestimmungen des „Schengener Durchführungsübereinkommen" errichtet wurde, stellt ein wichtiges Instrument für die Anwendung der Bestimmungen des - in den Rahmen der Europäischen Union einbezogenen - Schengen-Besitzstandes dar[14].

Das Schengener Informationssystem der zweiten Generation (kurz „SIS II") als ein System zur Suche, bzw. Fahndung nach Personen und Sachen - von Grenz-, Zoll-, Visa- und Strafverfolgungsbehörden im Schengen Raum genutzt - wird als C.SIS („Central Schengen Information System") im französischen Straßburg und als N.SIS („National Schengen Information System") in jedem Mitgliedsstaat betrieben.

Das jeweilige N.SIS besteht aus den nationalen Datensystemen, welche mit dem C.SIS kommunizieren. Die Gesamtheit aus C.SIS und der einzelstaatlichen N.SIS bilden das Schengener Informationssystem. Das österreichische N.SIS wird vom Bundesministerium für Inneres als Auftraggeber betrieben.

Die Einrichtung und Nutzung des Schengener Informationssystems der zweiten Generation ist in der sogenannten SIS II Verordnung Nr. 1987/2006[15] geregelt. Welche Personen und welche Dinge konkret im SIS II eingegeben und gespeichert werden dürfen, ist in Österreich in den §§ 33 ff. EU – Polizeikooperationsgesetzes 2009 (EU-PolKG)[16] normiert. Ausgeschrieben werden können demnach etwa zur Festnahme ausgeschriebene Personen, vermisste Minderjährige, Drittstaatsangehörige, die zur Einreiseverweigerung ausgeschrieben wurden oder gestohlene Gegenstände, Dokumente oder Waffen.

Dem Datenschutz widmet die SIS II Verordnung das Kapitel VI. (Recht auf Auskunft, Berichtigung und allenfalls Löschung unrechtmäßig gespeicherter Daten). Weiters sieht die SIS II Verordnung eine Aufsicht des jeweiligen N.SIS durch die nationalen Datenschutzbehörden vor mit einer individuellen Überprüfung der Datenverarbeitungsvorgänge alle vier Jahre. Dem Europäischen Datenschutzbeauftragten hingegen obliegt die Überwachung des C.SIS und der damit befassten Verwaltungsbehörde.

12 http://www.europoljsb.europa.eu/media/279967/16-25%20jsb%20opinion%20draft%20agreement%20europol%20georgia.pdf
13 http://www.europoljsb.europa.eu/media/280227/16-24%20jsb%20opinion%20draft%20agreement%20europol%20ukraine.pdf
14 Auszug aus Erwägungsgrund (1) der SIS II Verordnung Nr. 1987/2006 unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32006R1987&from=DE
15 Siehe http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32006R1987&from=DE
16 https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006630

Um hohe einheitliche Standards zu erreichen und das gegenseitige Vertrauen zwischen den Mitgliedstaaten zu stärken[17], wurde ein eigener Evaluierungs- und Überwachungsmechanismus zur Überprüfung der Anwendung des Schengen-Besitzstands mit der Verordnung Nr. 1053/2013 des Rates vom 7. Oktober 2013 eingeführt. Unter anderem nehmen Mitarbeiter der Datenschutzbehörde als nationale Experten an derartigen Evaluierungen teil. Im Berichtszeitraum hat die Datenschutzbehörde bei Evaluierungen in Italien, Malta und Frankreich mitgewirkt.

Die Datenschutzbehörde wird sich auch im Jahr 2017 an Evaluierungen beteiligen.

6.1.4 Zoll

Das gemeinsame Zollinformationssystem (ZIS) dient der Erfassung von Daten von Waren, Transportmittel, natürlichen und juristischen Personen, die im Zusammenhang mit Verstößen gegen das gemeinsame Zoll- und Agrarrecht stehen. Die Verarbeitung dieser Daten unterliegt der besonderen Kontrolle durch eine gemeinsame Kontrollinstanz, die aus Vertretern aller EU Datenschutzbehörden besteht, dem „Joint Supervisory Authority of Customs" (JSA. der durch das Übereinkommen über den Einsatz der Informationstechnologie im Zollbereich (ZIS)[18] eingerichtet wurde. Im Jahr 2016 wurde dem Rat der Abschlussbericht über die Prüfung des Europäischen Amts für Betrugsbekämpfung (OLAF) übermittelt.

Diese Kontrollinstanz war ursprünglich eine von drei durch den Rat der europäischen Union eingerichteten und vom Generalsekretariat des Rats fachlich und organisatorisch betreuten Kontrollinstanzen zur Überwachung 1.) des Schengener Informationssystems, 2.) von Europol und 3.) des Zollinformationssystems. Sowohl die fachliche Arbeit als auch die Sitzungen konnten daher effizient zusammengelegt werden. Mit 1. Mai 2017 wird nur mehr die gemeinsame Kontrollinstanz des Zollinformationssystems im fachlichen und organisatorischen Zuständigkeitsbereich des Rats verbleiben.

6.1.5 Eurodac

Das „Eurodac"-System ermöglicht den Einwanderungsbehörden der Mitgliedstaaten Asylwerber und andere Personen zu identifizieren, die beim illegalen Überschreiten einer EU-Außengrenze aufgegriffen werden. Anhand der Fingerabdrücke kann ein Mitgliedstaat feststellen, ob ein Fremder in einem anderen Mitgliedstaat Asyl beantragt hat oder ob ein Asylbewerber illegal in die EU eingereist ist. „Eurodac" besteht aus einer von der Europäischen Kommission verwalteten Zentraleinheit und den in den Mitgliedsstaaten zur Abfrage und Befüllung betriebenen nationalen Systemen. Art 32 der (EU) Verordnung Nr. 603/2013[19] sieht eine koordinierte Aufsicht und jährliche stichprobenartige Prüfung durch die nationale Datenschutzbehörde und die anderen EU Datenschutzbehörden mit dem Europäischen Datenschutzbeauftragten vor. Besonders hervorzuheben ist, dass die Europäische Kommission am 4.5.2016 einen Vorschlag zur Novellierung der Eurodac Verordnung veröffentlicht hat. In diesem „Recast Eurodac Regulation"[20] schlägt die Kommission unter anderem vor, den Kreis der Betroffenen auszuweiten, im Eurodac System mehr personenbezogene Daten zu erfassen, bessere Möglichkeiten zur Auswertung zu schaffen, die Daten länger zu speichern, das Mindestalter der zu erfassenden Personen von 14 auf 6 Jahre herabzusetzen, die Erfassung von Gesichtsbildern zu ermöglichen und ein zentrales Gesichts(wieder)erkennungssystem einzurichten. Dieser Vorschlag wird zur

17 Auszug aus dem Erwägungsgrund (3) der Verordnung Nr. 1053/2013 unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32013R1053&from=de
18 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=URISERV:l33046
19 http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32013R0603
20 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/proposal-implementation-package/docs/20160504/eurodac_proposal_en.pdf

Zeit im europäischen Parlament begutachet[21]. Der Europäische Datenschutzbeauftragte[22] und die Artikel 29 Datenschutzgruppe[23] haben dazu Stellung genommen.

6.1.6 Visa

Das Visa-Informationssystem (VIS) enthält Daten zu Ausstellungen, Ablehnungen, Annullierungen, Widerrufen und Verlängerungen von Kurzzeit-Visa in den Mitgliedstaaten des Schengen Raums. Rechtsgrundlage ist die Entscheidung 2004/512/EG des Rates und die Verordnung (EG) Nr. 767/2008[24]. Das System besteht aus einer von der EU als Auftraggeber betriebenen zentralen Datenbank und den nationalen Schnittstellen in den Schengen-Staaten, die der Befüllung und Abfrage der Datenbank dienen. Art. 43 der Verordnung sieht eine koordinierte Aufsicht durch die EU Datenschutzbehörden mit dem Europäischen Datenschutzbeauftragten vor. Art. 41 der Verordnung sieht eine individuelle Prüfung des VIS alle 4 Jahre durch die Datenschutzbehörde vor. In Erfüllung dieser Aufgabe hat die österreichische Datenschutzbehörde den österreichischen Auftraggeber des VIS (BMI) überprüft und eine Empfehlung ausgesprochen (siehe dazu auch Kapitel 3.2.7. des vorliegenden Berichtes).

6.2 Europarat

Die DSB vertritt die Republik Österreich im Ausschuss nach Art. 18 (T-PD) der Datenschutzkonvention des Europarates (EVS Nr. 108; BGBl. Nr. 317/1988). Im Berichtszeitraum fand von 29. Juni bis 1. Juli die 33. Plenarsitzung des T-PD in Straßburg statt. Die Tagesordnung sowie der zusammenfassende Bericht der Sitzung sind in englischer prache unter http://www.coe.int/en/web/data-protection/-consultative-committee-t-pd abrufbar.

Neben der Tätigkeit im T-PD war die Datenschutzbehörde auch in die innerstaatliche Koordination zur Vorbereitung der Verhandlungen hinsichtlich einer modernisierten Datenschutzkonvention eingebunden. Die entsprechenden Dokumente sind in englischer Sprache unter http://www.coe.int/en/web/data-protection/modernisation-convention108 abrufbar.

21 http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2016/0132%28COD%29&l=en#tab-0

22 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-09-21_CEAS_opinion_EN.pdf

23 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2016/20160929_letter_of_the_chair_of_the_art_29_wp_smart_boarders_en.pdf

24 http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32008R0767

7. Internationale Beziehungen

7.1. EU-US-Datenschutzschild (Privacy Shield)

Der Europäische Gerichtshof hat am 6. Oktober 2015, C-362/14, die Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärt. Auf Grundlage dieser Entscheidung war der Großteil des Datenverkehrs zwischen den Unternehmen in Mitgliedstaaten der Europäischen Union und den USA genehmigungsfrei.

Mit 12. Juli 2016 hat die Europäische Kommission den EU-US-Datenschutzschild (EU-US Privacy Shield) angenommen. Mit dieser Angemessenheitsentscheidung C(2016) 4176 final werden die Forderungen des Gerichtshof erfüllt, indem die Einführung eines Systems der Selbstzertifizierung erfolgte. Wurde ein Unternehmen zertifiziert, so ist der Datenfluss an dieses Unternehmen grundsätzlich genehmigungsfrei, das heißt, es ist keine Genehmigung der Datenschutzbehörde erforderlich. Im Rahmen der neuen Regelung wird das US-Handelsministerium die Liste der teilnehmenden Unternehmen regelmäßig überprüfen und aktualisieren, um sicherzustellen, dass die Unternehmen die Regeln einhalten, denen sie sich selbst unterworfen haben. Im Hinblick auf die Transparenz, Verwaltung sowie Überwachung des EU-US-Datenschutzschilds bestehen spezifische Überwachungs- und Durchsetzungsmechanismen. Halten Unternehmen die Regeln in der Praxis nicht ein, müssen sie mit Sanktionen und der Streichung von der Liste rechnen.

Das EU-US-Datenschutzschild bietet klare Schutzvorkehrungen und Transparenzpflichten beim Datenzugriff durch US-Behörden. Demnach ist ein Datenzugriff von Behörden aus Gründen der Rechtsdurchsetzung oder der nationalen Sicherheit nur unter Einhaltung klarer Beschränkungen, Schutzvorkehrungen und Aufsichtsmechanismen gestattet. Alle Personen in der EU erhalten erstmals Zugang zu Rechtsschutzmechanismen in diesem Bereich. Die USA haben eine unterschiedslose Massenüberwachung der im Rahmen des EU-US-Datenschutzschilds in die USA übermittelten personenbezogenen Daten ausgeschlossen. Das Büro des Direktors der nationalen Nachrichtendienste hat des Weiteren klargestellt, dass eine Sammelerhebung von Daten nur unter bestimmten Voraussetzungen und mit einer möglichst gezielten Ausrichtung erfolgen darf. Die Schutzvorkehrungen für die Verwendung von Daten unter solchen außergewöhnlichen Umständen werden im Einzelnen geregelt. Der US-Außenminister hat im Außenministerium eine Ombudsstelle eingerichtet, an die sich EU-Bürger mit Rechtsschutzbegehren, die den Bereich der nationalen Sicherheit betreffen, im Wege der jeweiligen nationalen Datenschutzbehörde wenden können.

Darüber hinaus stellt das EU-US-Datenschutzschild einen Schutzmechanismus für die Rechte des Einzelnen zur Verfügung. Ist ein EU-Bürger der Auffassung, dass seine Daten im Rahmen des Datenschutzschilds missbraucht wurden, stehen ihm mehrere Möglichkeiten der Streitbeilegung offen, von denen er Gebrauch machen kann. Idealerweise wird sich das Unternehmen selbst um die Beschwerde kümmern und das Problem lösen. Außerdem steht ein kostenloses Verfahren der alternativen Streitbeilegung zur Verfügung. Einzelpersonen können sich auch an ihre nationalen Datenschutzbehörden wenden, die dann zusammen mit der US-Handelskommission dafür sorgen, dass Beschwerden nachgegangen und abgeholfen wird. Kann der Fall nicht auf andere Weise gelöst werden, gibt es als letztes Mittel ein Schiedsverfahren.

Im Rahmen des EU-US-Datenschutzschilds wird ein jährlicher Überprüfungsmechanismus bereitgestellt. Überprüft wird dabei die Funktionsweise des Datenschutzschilds einschließlich der Zusicherungen und Zusagen hinsichtlich des Datenzugriffs aus Gründen der Rechtsdurchsetzung oder der nationalen Sicherheit. Die Europäische Kommission und das US-Handelsministerium sind gemeinsam an der Durchführung dieser Überprüfung beteiligt. Außerdem sind Sachverständige der US-Nachrichtendienste und der europäischen Datenschutzbehörden hinzuziehen. Die Kommission wird darüber hinaus alle anderen verfügbaren Informationsquellen heranziehen und einen an das Europäische Parlament und den Rat gerichteten öffentlichen Bericht vorlegen.