Republik Österreich
Datenschutz
behörde

Datenschutzbericht 2015

Datenschutzbericht 2015

Wien, im März 2016

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, 2016

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.

Der Restrukturierung der Behörde 2014 folgte im Jahr 2015 die Konsolidierung der neuen Strukturen und das gemeinsame Verständnis der Mitarbeiterinnen und Mitarbeiter von der Arbeit in den unterschiedlichen Bereichen wurde und wird von der Leitung forciert.

Der Datenschutzbericht 2015 ist der zweite, 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 Website 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 Welt des Datenschutzes.

Dr. Andrea Jelinek
Leiterin der Datenschutzbehörde

2 Die Datenschutzbehörde

2.1 Organisation und Aufgaben

2.1.1 Organisation

Mit 1. Jänner 2014 gingen die Aufgaben der Datenschutzkommission auf die Datenschutzbehörde über. Diese ist monokratisch strukturiert, aufgrund europarechtlicher und völkerrechtlicher Vorgaben unabhängig und keiner Dienst- und Fachaufsicht unterworfen.

Zur Leiterin der Datenschutzbehörde wurde Dr. Andrea Jelinek bestellt, zum stellvertretenden Leiter Dr. Matthias Schmidl. Beide wurden vom Bundespräsidenten auf Vorschlag der Bundesregierung 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 (bspw. eine Videoüberwachung oder Whistleblowing-System) 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.

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 unter http://www.dsb.gv.at/site/6189/default.aspx allgemeine Informationen zu den Verfahren vor der Datenschutzbehörde sowie Musterformulare für Eingaben zur Verfügung.

Informationen zum Meldeverfahren werden unter http://www.dsb.gv.at/DesktopDefault.aspx?alias=dvr 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. Die Bediensteten der Datenschutzbehörde sind in Erfüllung ihrer Aufgaben an die Weisungen der Leitung gebunden.

Erfreulicherweise ist es gelungen, den Personalstand im Jahr 2015 unter Nutzung der mobilitätsfördernden Maßnahmen für Mitarbeiterinnen und Mitarbeiter im Bundesdienst zu erhöhen.

Ob die Datenschutzbehörde aufgrund der Datenschutzgrundverordnung der Europäischen Union – die im Frühjahr 2016 beschlossen und 2 Jahre nach Beschlussfassung in Kraft treten wird – zusätzliche Mitarbeiterinnen und Mitarbeiter benötigen wird, kann zum jetzigen Zeitpunkt noch nicht mit abschließender Sicherheit gesagt werden. Klar ist jedenfalls, dass der Behörde neue Aufgaben zuwachsen werden, deren Erfüllung nicht durch den Wegfall des Datenverarbeitungsregisters (und der Arbeit in diesem Bereich) kompensiert werden kann. Der Personalbedarf wird auch davon abhängen, ob der Gesetzgeber (da die Verordnung teilweise in innerstaatliches Recht umgesetzt werden muss – sogenannte „hinkende Verordnung“) der Datenschutzbehörde all jene Aufgaben zuweisen wird, die laut Verordnung möglich sind. Ein etwaiger personeller Mehrbedarf wird jedenfalls rechtzeitig vor Inkrafttreten der Verordnung bekannt gegeben werden.

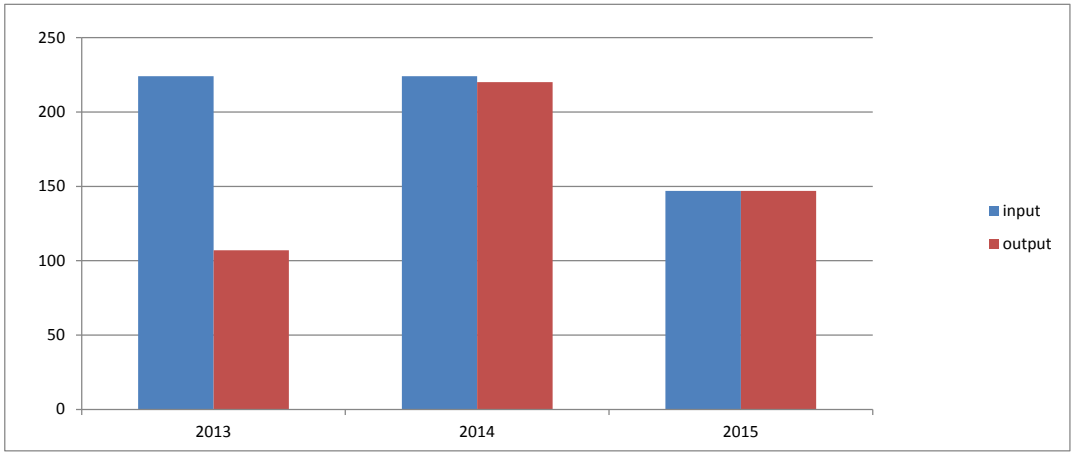
3 Tätigkeit der Datenschutzbehörde

3.1 Statistische Darstellung

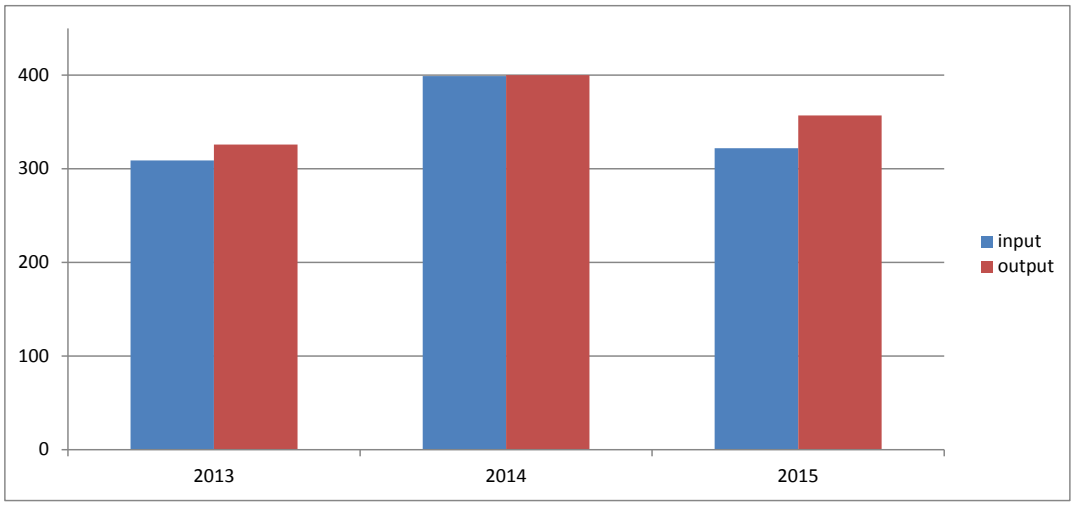
Tabelle 1 Anzahl der EIngangsstücke und Erledigungen, jeweils in den Jahren 2013, 2014 und 2015

	Eingangsstücke			Erledigungen		
Art der Tätigkeit	**2013**	**2014**	**2015**	**2013**	**2014**	**2015**
Individualbeschwerden	224	224	147	107	220	147
Erledigungsart der Individualbeschwerden	224	224	147	73 Bescheide 34 Einstellungen	117 Bescheide 103 Einstellungen	95 Bescheide 52 Einstellungen
Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (Verfahren über Antrag)	309	399	332	326	400	357
Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (amtswegiges Prüfverfahren)	79	98	67	80	88	97
Rechtsauskünfte	1133	2261	2152	1133	2261	2123
Genehmigungen nach § 46 und 47 DSG 2000 (wissenschaftliche Forschung u Statistik)	10	11	16	8	14	18
Genehmigungen im Internationalen Datenverkehr	48	79	128	41	80	150
Auskunft Schengen	42	33	10	39	33	7
Verfahren vor dem Bundesverwaltungsgericht		24	31			

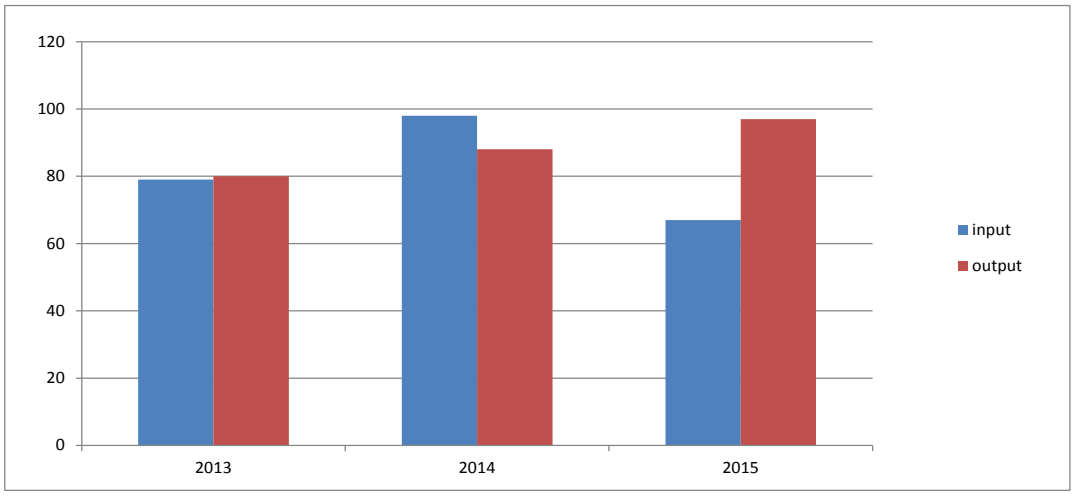
Individualbeschwerden § 31 DSG 2000



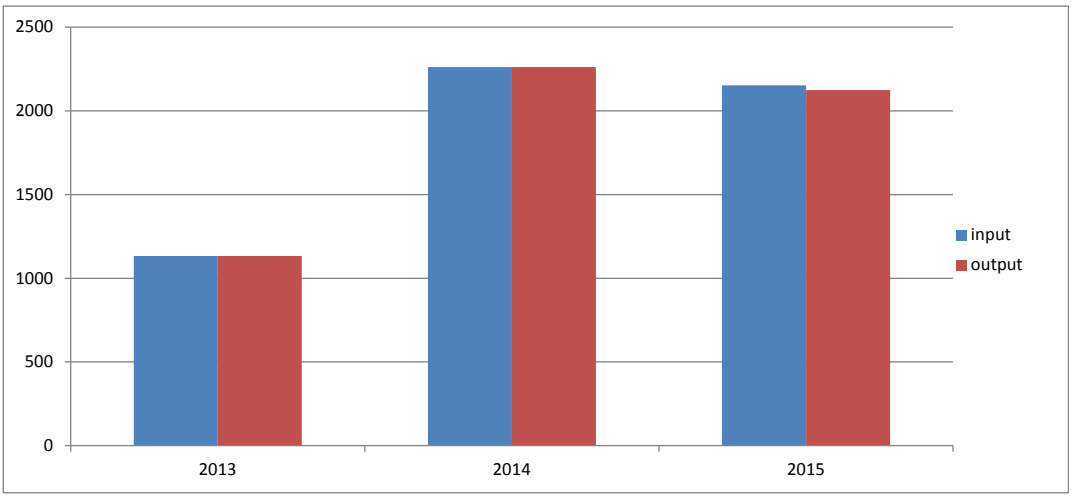
Kontroll- und Ombudsmannverfahren (§ 30 DSG 2000)



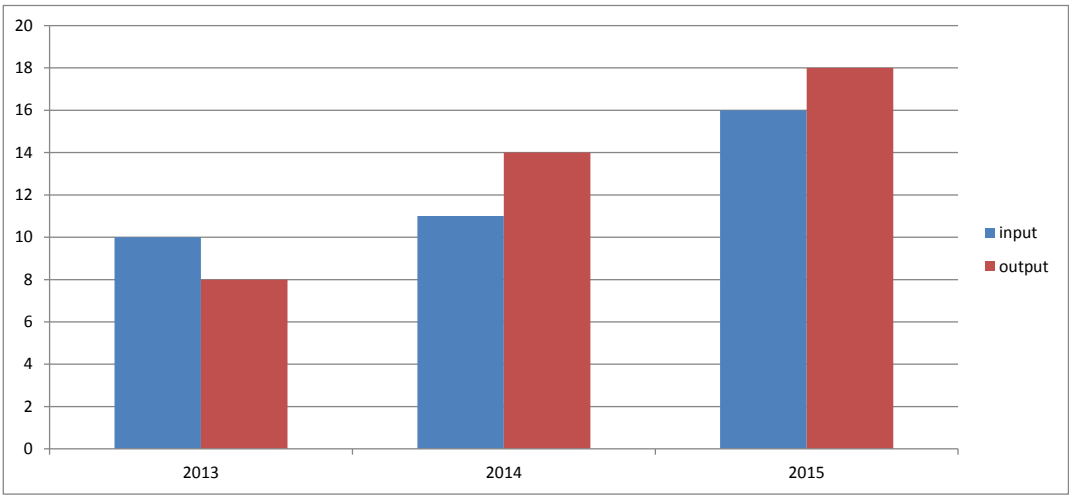
amtswegiges Prüfverfahren (§ 30 Abs. 2 DSG 2000)



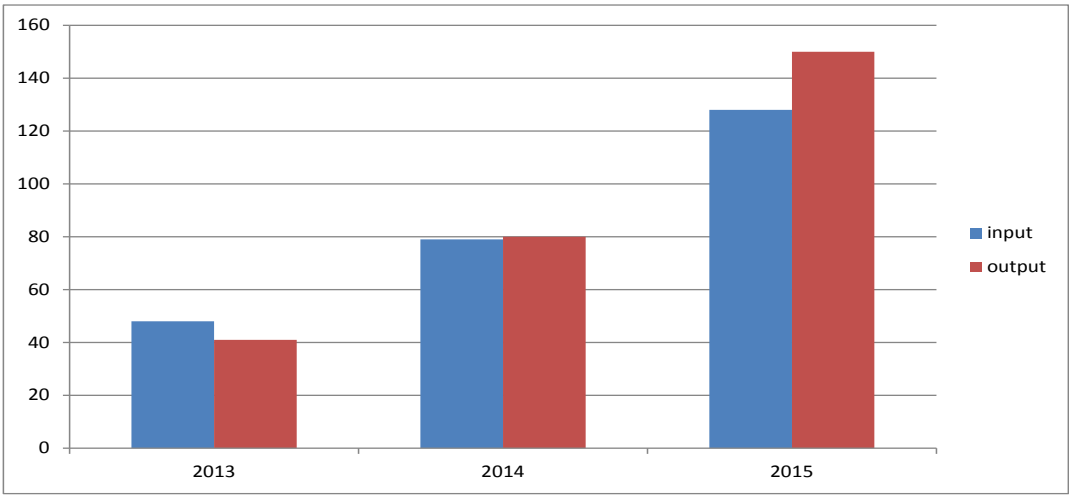
Rechtsauskünfte



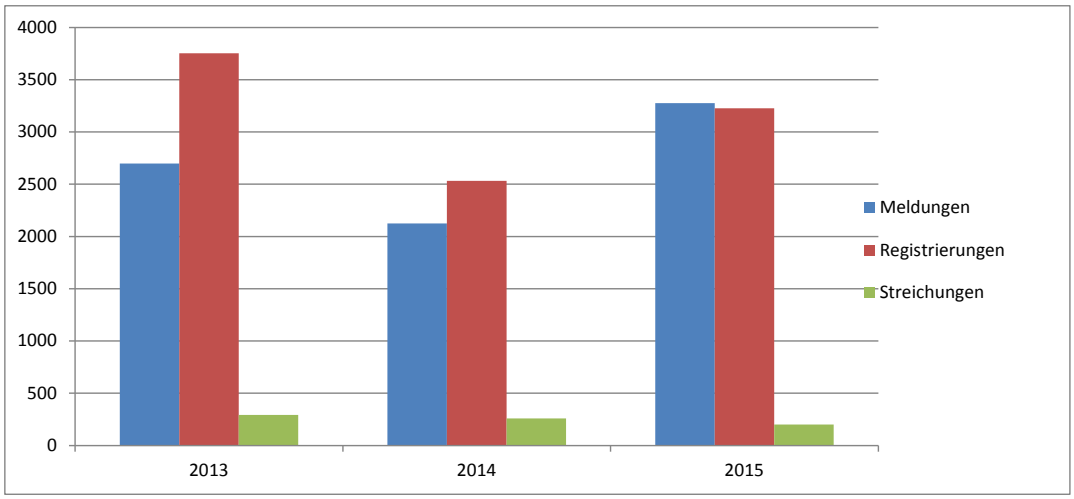
Genehmigung nach § 46 und 47 DSG 2000



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



Auftraggeber



Datenanwendungen

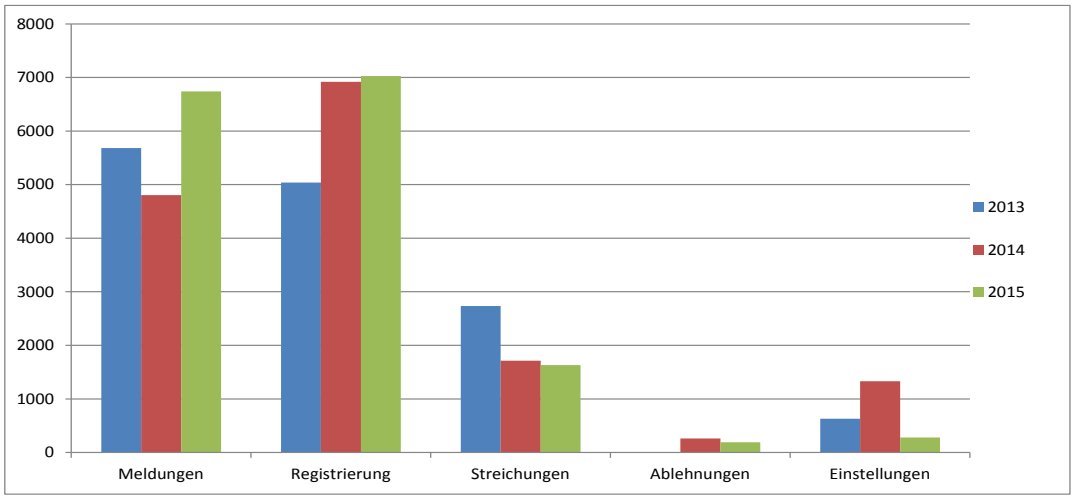


Tabelle 2 Anzahl der Tätigkeiten betreffend Datenverarbeitungsregister in den Jahren 2014 und 2015

Tätigkeiten	2013	2014	2015
Tätigkeiten für Auftraggeber in Summe	**5896**	**4918**	**6703**
Meldungen	2698	2125	3276
Registrierungen	2906	2533	3226
davon automatisch registriert	*1279 (ca. 44 %)*	*1188 (ca. 47 %)*	*2365 (ca. 73 %)*
davon durch das DVR registriert	*1627 (ca. 56 %)*	*1345 (ca. 53 %)*	*861 (ca. 27 %)*
Streichungen	292	260	201
Tätigkeiten in Datenanwendungen in Summe	**14088**	**15039**	**15872**
Meldungen	5681	4802	6741
davon automatisch registriert	*1488 (ca. 26%)*	*2340 (ca. 48 %)*	*3985 (ca. 59 %)*
davon vom DVR überprüft	*4193 (ca. 74%)*	*2462 (ca. 52 %)*	*2756 (ca. 41 %)*
Registrierungen	5040	6917	7028
Streichungen	2733	1712	1633
Ablehnungen	4	263	191
Einstellungen	630	1331	279
Verbesserungsaufträge in Summe	**1261**	**1175**	**1073**
Bescheide im Registrierungsverfahren	-	8	8
Verfahren gemäß § 22a DSG 2000	-	6	9
Rechtsunwirksam eingebrachte Meldungen	-	123	112
Meldungen von Rechtsnachfolgen	-	58	44

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. Gesetzgebung und Gerichtsbarkeit sind von der Zuständigkeit der Datenschutzbehörde ausgenommen.

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 hier 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 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 wird nicht durch einen in Form eines Bescheids ergehenden Verwaltungsakt sondern durch eine bloße Mitteilung entschieden. Diese bis auf die Schriftlichkeit nicht formgebundene Mitteilung des Auftraggebers ist daher nicht von den Verwaltungsgerichten sondern 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 Richtlinie 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 2015

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. Die datenschutzrechtlichen Leitthemen im Jahr 2015 waren das gesetzgeberische Vorhaben der EU-Datenschutz-Grundverordnung und der transatlantische Datentransfer, letzteres kulminierend im Safe-Harbor-Urteil des EuGH (siehe Punkt 4 des Berichts). Die Auswirkungen dieser Diskussionen auf das österreichische datenschutzrechtliche Beschwerdeverfahren, das auf den Bereich der innerstaatlichen öffentlichen Verwaltung und die Auskunftserteilung durch private Rechtsträger fokussiert ist, waren marginal.

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 bisher selten oder nie den Anstoß für ein gehäuftes Auftreten von typisierbaren Beschwerden (gleicher Inhalt, gleiche Adressaten) gegeben zu haben.

Aus den ersten Entscheidungen des Bundesverwaltungsgerichts ist vor allem abzuleiten, dass dem Ermittlungsverfahren ein hoher Aufwand zu widmen ist. In einem Beschwerdeverfahren eines Komplexes mehrerer Verfahren, der auch 2015 noch nicht abgeschlossen werden konnte, musste nach einer Bescheidbehebung durch das BVwG eine aufwändige und kostenintensive Beweisaufnahme durch einen nichtamtlichen Sachverständigen erfolgen, deren Kostenüberwälzung auf die Parteien (§ 76 Abs. 1 und 2 AVG, es geht dabei um Beträge in Höhe von mehreren Tausend Euro) nun einen weiteren Streitpunkt im fortgesetzten Verfahren bildet.

Die durch die DSG-Novelle 2010 eingeführte Möglichkeit, Beschwerdeverfahren als „gegenstandslos“ durch Einstellung zu beenden (§ 31 Abs. 8 DSG 2000), hat sich auch im Jahr 2015 als wesentlich für die Arbeit der Datenschutzbehörde erwiesen. 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 2015 konnten 52 Beschwerdeverfahren durch Einstellung (Beschwerdezurückziehungen aus anderen Gründen eingeschlossen) beendet werden. Die Praxis dieser Form der Verfahrensbeendigung wegen Klaglosstellung wurde und wird von mehreren Beschwerden gegen Bescheide der DSB in Frage gestellt (behauptet wird etwa ein rechtliches Interesse an der bescheidmäßigen Feststellung, dass die – faktisch unmöglich gewordene - Auskunft zu einem früheren Zeitpunkt erteilt hätte werden müssen, oder dass durch die verspätete Auskunftserteilung das Recht auf Auskunft verletzt worden ist), ist jedoch vom BVwG inzwischen in zwei Entscheidungen (Erkenntnisse vom 17.11.2015, W214 2014069-1 und W214 2107281-1) bestätigt worden.

Ausgewählte Beschwerdeentscheidungen aus 2015

Die Datenschutzbehörde hat in ihrer öffentlich zugänglichen Entscheidungsdokumentation (im Rahmen des Rechtsinformationssystems des Bundes – RIS; Stand: 19. Februar 2016) für 2015 elf Bescheide aus Beschwerdeverfahren dokumentiert. Diese Zahl kann sich aus verschiedenen Gründen (z.B. wegen abzuwartender Rechtsmittelentscheidungen des BVwG, VfGH oder VwGH) auch nach Erscheinen des Datenschutzberichts 2015 noch ändern.

Durch die Etablierung des Bundesverwaltungsgerichts als Rechtsmittelinstanz ist die Bedeutung der Rechtsprechung der Datenschutzbehörde für die verbindliche Auslegung und Weiter-

entwicklung des Datenschutzrechts reduziert worden. Regelmäßig werden daher nur rechtskräftige Entscheidungen dokumentiert, Ausnahmefälle sind in den RIS-Dokumenten durch entsprechende Vermerke gekennzeichnet. In solchen 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 8.1.2015, DSB-D122.196/0012-DSB/2014 (Veröffentlichung einer Disziplinarentscheidung einer Standesorganisation)

Der Beschwerdeführer wurde vom Tiroler Jägerverband (Beschwerdegegner) als Jäger wegen eines verbotenen Abschusses disziplinarrechtlich bestraft und diese Disziplinarentscheidung unter Angabe von Name und Adresse in der Verbandszeitschrift, die auch als Online-Ausgabe bei Beschwerdeerhebung in diesem Umfang allgemein verfügbar war, veröffentlicht. Die DSB kam zu dem Schluss, dass die Bestimmung des Tiroler Jagdrechts (§ 68 Abs. 3 TJG 2004), auf die sich der Beschwerdegegner berufen hatte, weder eine ausreichend präzise Ermächtigung zum Eingriff in das Recht auf Geheimhaltung darstellt, noch die namentliche Veröffentlichung hier dem Grundsatz des gelindesten Mittels entsprach. Daher wurde ein unzulässiger Eingriff in das Recht auf Geheimhaltung festgestellt (hinsichtlich der begehrten Löschung war die Disziplinarentscheidung während des laufenden Verfahrens aus der Online-Ausgabe entfernt worden, ein Antrag auf Erteilung eines entsprechenden Leistungsauftrags wurde generell als im öffentlichen Bereich unzulässig zurückgewiesen).

b) Bescheid vom 9.2.2015, DSB-D122.244/0001-DSB/2015 (Löschung erkennungsdienstlicher Daten)

Der Beschwerdeführer war unter dem Verdacht des versuchten Betruges im Jahr 2013 im Zuge der kriminalpolizeilichen Ermittlungen erkennungsdienstlich behandelt worden. Die Daten (Fingerabdrücke, Fotos) wurden im Auftrag der Sicherheitsbehörde (Landespolizeidirektion Oberösterreich) verwendet. Das Strafverfahren wurde nach Diversion (Zahlung einer Geldbuße) durch das Gericht eingestellt. Die vom Beschwerdeführer verlangte Löschung der erkennungsdienstlichen Daten wurde von der Sicherheitsbehörde im August 2014 abgelehnt. Die datenschutzrechtliche Beschwerde dagegen war erfolgreich, da die Sicherheitsbehörde als Grund für die weitere Speicherung der Daten keine deliktspezifische Rückfallsgefährdung („aufgrund der Art oder Ausführung der Tat oder der Persönlichkeit des Betroffenen“) nachweisen konnte. Die Darlegung der allgemein abschreckenden Wirkung erkennungsdienstlicher Datenverarbeitung auf potenzielle Täter reicht in einem solchen Fall nicht aus. Eine ähnliche gelagerte Entscheidung erging im Bescheid vom 10.3.2015, DSB-D122.211/0002-DSB/2015.

c) Bescheid vom 3.3.2015, DSB-D122.272/0004-DSB/2014 (Auskunftsrecht, Mitwirkungsobliegenheit des Betroffenen, Zeitaufwand)

Im Zuge des Verfahrens zur Erteilung einer datenschutzrechtlichen Auskunft ersuchte eine Bezirksverwaltungsbehörde den Beschwerdeführer, sein Verlangen nach Auskunft über „alle Daten“ dadurch zu präzisieren, dass er aus einer Liste von 38 Datenanwendungen eine Auswahl treffe. Der Beschwerdeführer verweigerte dies. Die Bezirksverwaltungsbehörde lehnte als datenschutzrechtlich Verantwortliche daraufhin die inhaltliche Auskunftserteilung mangels ausreichender Mitwirkung ab. Die dagegen erhobene datenschutzrechtliche Beschwerde blieb erfolglos. Die DSB erachtete die Vorgehensweise der Bezirksverwaltungsbehörde für rechtmäßig, da „der Beschwerdeführer seiner Mitwirkungspflicht gemäß § 26 Abs. 3 DSG 2000 nicht im vom Gesetzgeber geforderten zumutbaren Ausmaß nachgekommen ist, sodass eine Suche

in allen 38 Datenanwendungen des Beschwerdegegners – auch unter dem Gesichtspunkt des fehlenden zentralen Zugriffs auf alle ihre Datenanwendungen im Zusammenhalt mit dem dargelegten Zeiterfordernis – wohl nur mit einem ungerechtfertigten und unverhältnismäßigen Aufwand verbunden wäre." Die DSB ging dabei von einer Abfragedauer von sechs Minuten je Datenanwendung und damit einem Gesamtzeitaufwand von knapp vier Stunden aus.

Eine ähnliche gelagerte Entscheidung erging im Bescheid vom 3.3.2015, DSB-D122.273/0002-DSB/2015, wobei dort der datenschutzrechtlich Verantwortliche das Amt der Steiermärkischen Landesregierung mit 106 Datenanwendungen war.

d) Bescheid vom 9.3. 2015, DSB-D122.299/0003-DSB/2015 (Auskunftspflicht eines Rechtsanwalts, Verschwiegenheitspflicht)

Im Zuge des Verfahrens zur Erteilung einer datenschutzrechtlichen Auskunft hatte der datenschutzrechtlich Verantwortliche, ein Rechtsanwalt, die inhaltliche Auskunftserteilung ohne nähere Begründung unter Verweis auf die anwaltliche Verschwiegenheitspflicht gemäß § 9 Abs. 2 RAO abgelehnt. Die dagegen erhobene datenschutzrechtliche Beschwerde war erfolgreich. Die DSB hielt unter Verweis auf vorliegende Rechtsprechung der früheren DSK fest, dass aus der Begründung der Ablehnung für den Betroffenen selbst, jedoch auch für die Datenschutzbehörde, nachvollziehbar hervorgehen muss, aus welchen überwiegenden Gründen keine Auskunft erteilt wird.

e) Bescheid vom 11.3.2015, DSB-D122.319/0002-DSB/2015 (Datenschutzrechte eines aufgelösten Vereins)

Der Beschwerdeführer, ein Branchenverband, bei dem der Betroffene, ein nach Selbstauflösung nicht mehr existierender Verein, Mitglied war, versuchte unter Berufung auf ein früheres Löschungsverlangen des Betroffenen an die Finanzmarktaufsichtsbehörde (FMA) mit Beschwerde wegen Verletzung des Rechts auf Löschung gegen die FMA vorzugehen. Bei den zu löschenden Daten handelte es sich um eine Warnmeldung auf der Website der FMA wegen unbefugter Ausübung von Versicherungsgeschäften. Die DSB wies die Beschwerde ab bzw. zurück, da der Beschwerdeführer nicht Betroffener der Warnmeldung war, und die Datenschutzrechte des aufgelösten Vereins mit dem Erlöschen von dessen Rechtspersönlichkeit ebenfalls erloschen sind. Ein Übergang dieser persönlichen Rechte auf Rechtsnachfolger kommt auch bei einer juristischen Person generell nicht in Frage.

f) Bescheid vom 27.4.2015, DSB-D122.257/0003-DSB/2015 (Rechtsschutz, kriminalpolizeiliche Datenverwendung)

Der Beschwerdeführer, der zeitweilig und unbegründet unter Verdacht gestanden hatte, an Suchtgiftgeschäften beteiligt zu sein, behauptete eine Verletzung im Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten in Folge telefonischer Bekanntgabe seiner Ladung zur polizeilichen Einvernahme an seinen Arbeitgeber. Die datenschutzrechtlich verantwortliche Sicherheitsbehörde (Bezirkshauptmannschaft) bestritt als Beschwerdegegnerin die Zuständigkeit der DSB. Die DSB wertete die von einem Beamten gesetzten Schritte als Erkundigungen und als eine Ladung zur Vernehmung des Beschwerdeführers, somit als Maßnahmen im Sinne der §§ 152ff StPO, die wiederum gemäß § 91 Abs. 2 StPO der Gewinnung, Sicherstellung, Auswertung oder Verarbeitung einer Information zur Aufklärung des Verdachts einer Straftat dienten (kriminalpolizeiliches Handeln). Gegen diese verwaltungsbehördlichen Akte (eine Anordnung einer Staatsanwaltschaft oder eines Gerichts lag nicht vor) „im Dienste der Gerichtsbarkeit" stellt § 106 StPO inzwischen wieder die Möglichkeit des Einspruchs bei Gericht zur Verfügung

(keine Rechtschutzlücke). Die DSB folgte daher den Einwänden der Beschwerdegegnerin und wies die Beschwerde wegen Unzuständigkeit zurück.

Durch das Erkenntnis des Verfassungsgerichtshofs (VfGH) vom 30. 6. 2015, G 233/2014 ua, ist jedoch neuerlich, wirksam ab 1. 8. 2016, die Bestimmung über die Zuständigkeit der Gerichte für Einsprüche gegen kriminalpolizeiliche Ermittlungsmaßnahmen als verfassungswidrig aufgehoben worden.

g) Bescheid vom 10.7.2015, DSB-D122.331/0005-DSB/2015 (Fußballsport, Gefährderdaten, Datenaustausch Sicherheitsbehörde – Bundesliga)

Der Beschwerdeführer wandte sich wegen Verletzung seines Rechts auf Geheimhaltung gegen die Bezirkshauptmannschaft Salzburg-Umgebung als Sicherheitsbehörde und brachte vor, diese habe im Zusammenhang mit einer erstatteten Strafanzeige (gewalttätige Ausschreitungen gegen Polizeibeamte bei einem Fußballspiel am 5.10.2013, Verdacht des Widerstandes gegen die Staatsgewalt und versuchter schwerer Körperverletzung, Strafverfahren im Zeitpunkt des Beschwerdeverfahrens offen) seine Daten (Name, Geburtsdatum, Wohnanschrift sowie Angaben zum Grund und maßgebliche Umstände des Einschreitens bei dem erwähnten Fußballspiel) unberechtigt an den Verein Österreichische Fußball-Bundesliga übermittelt. Die DSB wies die Beschwerde ab und hielt fest, dass sich die Übermittlung auf die ausdrückliche Ermächtigung dazu in § 56 Abs. 1 Z 3a SPG stützen kann. Zwar sei es gesetzwidrig unterlassen worden, den Beschwerdeführer davon zu verständigen, dies hatte jedoch auf die Rechtmäßigkeit der Übermittlung keine Auswirkung. Auch eine Entscheidung im gerichtlichen Strafverfahren musste dazu nicht abgewartet werden.

h) Bescheid vom 7.8.2015, DSB-D122.311/0007-DSB/2015 (Vorlage von Beweisurkunden als Datenübermittlung, Zivilprozess, Behördenbegriff)

Das Dienstverhältnis der Beschwerdeführerin als bei einem Sozialversicherungsträger angestellter Zahnärztin war durch Entlassung beendet worden. Angegebener Grund war die Abwerbung von Patienten des Kassenambulatoriums für die Privatpraxis der Beschwerdeführerin. Die Entlassung wurde beim Arbeitsgericht angefochten. Der Sozialversicherungsträger (Beschwerdegegner) legte im Prozess dem Gericht Kopien von Honorarnoten als Beweismittel vor, die die Beschwerdeführerin in ihrer Privatpraxis ausgestellt hatte, und die von Patienten zur Refundierung der Behandlungskosten beim Sozialversicherungsträger eingereicht worden waren. Die Beschwerdeführerin sah darin eine Verletzung ihres Rechts auf Geheimhaltung. Die Beschwerde wurde jedoch abgewiesen, da sich das Vorgehen des Sozialversicherungsträgers auf den Rechtfertigungsgrund gemäß § 8 Abs. 3 Z 5 DSG 2000 („Verwendung der Daten...zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde“) stützen konnte. Die DSB hielt – entgegen dem Vorbringen der Beschwerdeführerin – fest, dass der Begriff der „Behörde“ im DSG 2000 sowohl Verwaltungsbehörden wie auch Gerichte umfasst.

3.2.2 Kontroll- und Ombudsmannverfahren

Im sogenannten 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) bzw. 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 200 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 aber auch ohne Einsatz dieses Mittels erreicht werden.

Die zahlenmäßig größte Gruppe von Eingaben betraf, wie in den Vorjahren, Fragen der Videoüberwachung. Hervorzuheben ist jedoch auch der im Berichtszeitraum ergangene Mandatsbescheid betreffend Videoüberwachung, in welchem abermals festgehalten wurde, dass eine Videoüberwachung hinsichtlich allgemein zugänglicher Flächen in einem Mehrparteienwohnhaus etwa zur Abschreckung von Einbrechern (Schutzzweck) oder zur Identifizierung eines Sachbeschädigers (Beweissicherungszweck) zulässig sei, nicht jedoch, um mit Hilfe der Videoüberwachung Beweise für eine vertragswidrige Nutzung des Mietgegenstandes (z.B. Nichtgebrauch, unerlaubte Untervermietung) zu sammeln oder ganz allgemein Daten zum Privatleben der Mieter zu erheben.

Im Berichtszeitraum scheinen des Weiteren die folgenden Fälle besonders erwähnenswert:

a) Empfehlung zur Durchführung einer Befragung über arbeitsbedingte psychische Belastungen mit anschließender Auswertung (DSB-D215.611/0003-DSB/2014, 30. März 2015)

Die datenschutzrechtliche Auftraggeberin führte im Jahr 2014 eine Onlinebefragung über arbeitsbedingte psychische Belastungen durch. Bei der auf freiwilliger Basis erfolgten Teilnahme an der Umfrage musste jeder Teilnehmer u.a. seine Arbeitsstätte, sein Geschlecht und sein Alter angeben. Die Auftraggeberin besteht aus zwei Abteilungen, in welchen insgesamt nur vier männliche Personen unter 35 Jahren arbeiten. Die Rücklaufquote der Umfrage betrug 20%. Bei der Präsentation der Ergebnisse gab der Einschreiter indirekt zu, an der Umfrage teilgenommen zu haben. Die Evaluierung der Umfrage zeigte, dass nur eine männliche Person unter 35 Jahren teilnahm und diese sich tendenziell negativ über die Arbeitsbedingungen äußerte.

Die DSB verwies zur Frage, wie eine Auswertung unter Wahrung der Anonymität vorzunehmen sei und wie viele Personen eine Gruppe umfassen sollte, im Wesentlichen auf die Empfehlung der Datenschutzkommission vom 22. Mai 2013, GZ K213.180/00031-DSK/2013. Ausgehend davon hielt die DSB fest, dass eine Befragung über arbeitsbedingt psychische Belastungen so zu gestalten sei, dass durch die Auswertung der Ergebnisse oder aber auch durch die direkt oder indirekt zugegebene bloße Teilnahme an einer Befragung einen Rückschluss auf bestimmte Arbeitnehmer nicht möglich sei.

Die DSB empfahl, die Auftraggeberin möge geeignete Maßnahmen ergreifen, um sicherzustellen, dass auf Grund einer Befragung über arbeitsbedingte psychische Belastungen und der anschließenden Auswertung ein Personenbezug zu einzelnen Mitarbeitern eines Unternehmens nicht möglich sei.

b) Empfehlung zur unzulässigen Übermittlung einer Hausverbotsliste (DSB-D215.529/0002-DSB/2015, 1. April 2015)

Der Einschreiter ist deklarierter Fan der Fußballmannschaft FC E und war als Stammkunde der FC E-AG unter anderem Inhaber einer Dauerkarte für das E-Stadion. Mit Schreiben der FC E-AG vom 11. Februar 2014 wurde über den Einschreiter bis zum 12. Februar 2016 ein Hausverbot „in und auf allen Liegenschaften des FC E“ verhängt. Eine Meldung des Hausverbots an die Bundesliga oder eine entsprechende Datenübermittlung ist jedoch nicht erfolgt. Auch bestand gegen den Einschreiter kein von der Bundesliga ausgesprochenes, für alle teilnehmenden Spielveranstalter satzungsgemäß bindendes, ligaweites Stadionverbot. Allerdings wurde dem Einschreiter auch bei Auswärtsspielen des FC E der Eintritt in das Stadion verwehrt, nachdem Verbindungspersonen (sogenannte „Fanordner“) der FC E AG mit Zugang zu den Daten der Datenanwendung der Auftraggeberin FC E AG „Datei zur Festlegung und Aussprache örtlicher Hausverbote und zur Festlegung von bundesweiten Stadionverboten“ (in Form einer ausgedruckten Liste) den Einschreiter bei der Einlasskontrolle identifiziert und gegenüber dem Sicherheitspersonal des jeweiligen Spielveranstalters als mit Hausverbot belegte Person bezeichnet hatten.

Die DSB hielt zunächst fest, dass das Faktum, dass die FC E AG den Einschreiter kraft ihres Hausrechts durch einseitige Willenserklärung vom Betreten ihrer Anlagen ausgeschlossen habe (Verhängung des Hausverbots), feststehe und in seiner Rechtmäßigkeit von der Datenschutzbehörde nicht überprüft werde. Ein Veranstalter von Sportveranstaltungen oder ähnlichen „Events“ sei jedenfalls grundsätzlich berechtigt, solche Verbote auszusprechen. Als Veranstalterin von Fußballspielen im E-Stadion und somit das Hausrecht Ausübende sei die FC E AG auch rechtlich befugt (gewesen), Daten für den Zweck der effektiven Durchsetzung des über den Einschreiter verhängten Hausverbots zu verarbeiten. Allerdings wirke das Hausverbot, anders als ein von der Bundesliga als Organisator des Wettbewerbs ausgesprochenes Stadionverbot, an das alle Teilnehmer der Liga gebunden wären, nur innerhalb der Grenzen des Hausrechts der FC E AG, weshalb der Einschreiter durch die gegenständliche erfolgte Datenübermittlung, in seinem Recht auf Geheimhaltung personenbezogener Daten verletzt worden sei. Die Übermittlung von Daten sei nämlich nicht auf das automationsunterstütze, digitale, elektronische oder sonst maschinelle Übertragen von Informationen und Zeichen beschränkt. Selbst eine Geste in Richtung einer bestimmten Person, ausgeführt durch einen „Fanordner“ mit dem allen Beteiligten bekannten, durch das Abfragen und Einsehen der Hausverbotsliste hergestellten Wissen, dass gegen eine solcherart bezeichnete Person im Heimstadion des FC E ein Hausverbot gelte, sei daher eine Datenübermittlung. Im Übrigen habe der datenschutzrechtliche Auftraggeber FC E AG auch keinerlei Datenübermittlung aus der gegenständlichen Datenanwendung an andere Auftraggeber gemeldet und im DVR publiziert.

Die DSB empfahl, die Auftraggeberin möge die von ihr gemeldete Datenanwendung mit der Bezeichnung „Datei zur Festlegung und Aussprache örtlicher Hausverbote und zur Festlegung von bundesweiten Stadionverboten“ im Hinblick auf Datenübermittlungen überprüfen und gegebenenfalls Betroffene, die zu übermittelnden Datenarten und die zugehörigen Empfängerkriese ergänzen. Jedenfalls bis zur Offenlegung entsprechender Datenübermittlungen möge jede Übermittlung von Daten aus der genannten Datenanwendung unterlassen werden.

c) Empfehlung wegen Änderung der Rechtsform samt Namen und Wegfall des Zwecks und Rechtsgrundlage der Datenanwendung (DSB-D215.814/0003-DSB/2015, 1. Juli 2015)

Die Auftraggeberin war noch unter der seit 8. Dezember 2012 (Umwandlung der Aktiengesellschaft in eine Gesellschaft mit beschränkter Haftung) namentlich geänderten Firma und der

Rechtsform einer Aktiengesellschaft unter der betreffenden DVR-Nummer im DVR eingetragen. Des Weiteren hat die Auftraggeberin am 30. September 2012 eine Datenanwendung mit der Bezeichnung „Verarbeitung und Speicherung von Vorratsdaten gemäß § 102aff iVm § 94 TGK iVm DSVO sowie Übermittlung in verschlüsselten und gesicherten Dateiformaten an die Strafverfolgungs- und Sicherheitsbehörden über die Durchlaufstelle gemäß DSVO“ der früheren Datenschutzkommission gemeldet, die am 26. Mai 2014 von der Datenschutzbehörde im DVR registriert wurde. Gemäß der am 30. Juni 2014 erfolgten Kundmachung des Bundeskanzlers über die Aufhebung von Bestimmungen des Telekommunikationsgesetzes 2003, der Strafprozessordnung 1975 und des Sicherheitspolizeigesetzes durch den Verfassungsgerichtshof, BGBl. I Nr. 44/2014, endete die Pflicht der Auftraggeberin, Vorratsdaten zu speichern, mit Ablauf des Tages der Kundmachung.

Die DSB erkannte in ihrer Entscheidung, dass die Auftraggeberin zweimal ihre datenschutzrechtliche Meldepflicht gemäß § 17 Abs. 1 DSG 2000 vernachlässigt habe. Schließlich habe jeder datenschutzrechtliche Auftraggeber jederzeit für die Richtigkeit und Vollständigkeit aller ihn betreffenden Daten im DVR, wie diese als Inhalte des DVR in den Anlagen 1 bis 3 zu DVRV 2012 vorgesehen sind, einstehen müsse. Änderungen müsse er unverzüglich selbst gemäß § 17 Abs. 1a DSG 2000 über die Internetanwendung DVR-Online melden und dürfe sich dabei nicht darauf verlassen, dass der Datenschutzbehörde Änderungen gemäß § 22 Abs. 2 DSG 2000 bekannt werden, oder dass die Datenschutzbehörde auf bloßen Verdacht hin entsprechende Ermittlungen anstelle und amtswegig Richtigstellungen im DVR vornehme. Dies gelte hier zunächst für Änderungen der Rechtsform und damit der Firma einer Kapitalgesellschaft. Des Weiteren, so die DSB, diene das DVR insbesondere der „Publizität der Datenanwendungen (Überschrift des 4. Abschnitts des DSG 2000 vor § 16). Darunter sei zu verstehen, dass das DVR jedermann ein wahrheitsgemäßes, der Realität der meldepflichtigen Datenverwendung durch einen datenschutzrechtlichen Auftraggeber bestmöglich angenähertes Bild bieten solle. Derzeit erwecke der Stand des DVR den Eindruck, die Auftraggeberin würde weiterhin die Vorratsdatenspeicherung vollziehen, was einen gesetzwidrigen Eingriff in das Grundrecht auf Datenschutz einer Vielzahl von Personen darstellen würde. Datenanwendungen, die ausschließlich einem speziellen, gesetzlich festgelegten Zweck dienten, seien daher nach Wegfall dieses Zwecks bzw. der Rechtsgrundlage unverzüglich durch Änderungsmeldung gemäß § 22 Abs. 1 DSG 2000 zu streichen.

Die DSB empfahl, die Auftraggeberin möge durch eine Änderungsmeldung die Datenanwendung mit der Bezeichnung „Verarbeitung und Speicherung von Vorratsdaten gemäß § 102aff iVm § 94 TGK iVm DSVO sowie Übermittlung in verschlüsselten und gesicherten Dateiformaten an die Strafverfolgungs- und Sicherheitsbehörden über die Durchlaufstelle gemäß DSVO“, aus dem DVR streichen lassen und ihre Bezeichnung (Firma) im DVR in näher bezeichneter Weise ändern oder eine entsprechende, firmenrechtlich zulässige Abkürzung richtigstellen.

3.2.3 Rechtsauskünfte an Bürgerinnen und Bürger

Die Datenschutzbehörde stellt auf ihrer Homepage umfassende Rechtsinformationen in Zusammenhang mit dem DSG 2000 zur Verfügung http://www.dsb.gv.at/site/6175/default.aspx . 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

An der grundsätzlichen Struktur der Anträge zur Genehmigung für den internationalen Datenverkehr hat sich im Berichtszeitraum wenig geändert. Sie stammen ausschließlich von Konzernunternehmen in Österreich. Auch der Inhalt der Anträge (Personalverwaltung und Kunden- bzw. Lieferantenverwaltung) ist gleichartig.

Im Jahr 2013 wurden die ersten Genehmigungen mit verbindlichen unternehmens-internen Vorschriften (Binding Corporate Rules, kurz BCR) als rechtliche Instrumente zur Wahrung der schutzwürdigen Geheimhaltungsinteressen der Betroffenen erteilt. Im Jahr 2014 gab es weitere Genehmigungen auf der Grundlage von BCR's, und dieser Trend hat sich 2015 fortgesetzt. Im Berichtszeitraum wurden hauptsächlich Standardvertragsklauseln als rechtliche Instrumente eingesetzt, aber BCR's scheinen sich als Alternative etabliert zu haben.

Der Einsatz von Dienstleistern mit Cloud-Technologie war ein neues Thema für die Datenschutzbehörde. Die ersten Entscheidungen gehen in die Richtung, dass Cloud-Dienstleistungen zulässig sind, sofern das erforderliche datenschutzrechtliche Sicherheitsniveau garantiert werden kann.

Für den Datenverkehr zwischen der EU und den USA bestand eine besondere Regelung, der „Safe Harbor". Danach war die Übermittlung und Überlassung an amerikanische Unternehmen, die Mitglied im Safe Harbor waren, genehmigungsfrei. Im Gegensatz zu anderen Angemessenheitsentscheidungen der Europäischen Kommission galt diese Privilegierung des Datenverkehrs nicht für das ganze Land, sondern nur für Unternehmen in den USA, die sich selbst zur Einhaltung bestimmter Datenschutzregeln verpflichtet hatten. Nach der Ungültigerklärung der Safe Harbor-Entscheidung der Europäischen Kommission durch den EuGH am 6. Oktober 2015 hat die Datenschutzbehörde einige Anträge von Unternehmen erhalten, die bisher auf der Grundlage von Safe Harbor genehmigungsfrei personenbezogene Daten in die USA exportieren konnten.

3.2.5 Registrierungsverfahren

Die Datenschutzbehörde hat im Jahr 2014 ein Verfahren zur effizienteren Registrierung von Whistleblower-Systemen (Hinweisgebersystemen) entwickelt. Dieses baut auf der Regelung in § 19 Abs. 2 DSG 2000 auf, wonach ein Auftraggeber zusagen kann, dass er beim Betrieb einer Datenanwendung bestimmte Auflagen oder Bedingungen beachten wird. Nach der Judikatur zu den Whistleblower-Fällen wurde ein einheitlicher Katalog von Auflagen entwickelt, der den Meldungslegern zur Verfügung gestellt wird. Wenn diese bereit sind, die vorgegebenen Auflagen zu akzeptieren, kann ohne Erlassung eines Bescheides registriert werden.

Die Datenschutzbehörde hat gute Erfahrungen mit dieser Methode gemacht und setzt sie regelmäßig ein.

In mehreren Fällen wurde diese Registrierung gemäß § 19 Abs. 2 DSG 2000 von der Datenschutzbehörde dem Auftraggeber angeboten, der jedoch keine Position bezogen hat, also weder angenommen noch abgelehnt hat. Dies wurde regelmäßig mit Problemen der Koordination innerhalb des Konzerns begründet. Der Effekt, nämlich die raschere Abwicklung für den Auftraggeber, kann in solchen Fällen nicht zum Tragen kommen. Die Datenschutzbehörde erwägt, in solchen Fällen mit Bescheid zu registrieren und dabei dieselben Auflagen zu setzen, die auch bei einer Zusage gemäß § 19 Abs. 2 DSG 2000 zum Tragen gekommen wären.

Registrierungen:

a. Aufgrund einer rechtlichen Neubewertung wurden zahlreiche Meldungen von Skiliftbetreiber-Gesellschaften hinsichtlich der Datenanwendung „Photocompare“ nunmehr außerhalb des Videoüberwachungsregimes der §§ 50a ff DSG 2000 als Zutrittskontrollsystem registriert (vgl. dazu den Datenschutzbericht der Datenschutzbehörde aus dem Jahr 2014, Seite 19, Pkt. 3.2.5.a). Der Zweck ist dabei abweichend von Videoüberwachungsanlagen nicht auf den Schutz eines überwachten Objekts gerichtet, sondern ausschließlich auf die Kontrolle des Zutrittes zur Liftanlage. Rechtsgrundlage für die Datenanwendung sind überwiegende berechtigte Interessen der Auftraggeber resultierend aus ihrer Verpflichtung zur Vertragserfüllung gegenüber den Kunden (Beförderungsvertrag). Darüber hinaus entscheidend für den rechtmäßigen Betrieb von Photocompare-Anlagen ist die ausführliche Information der Betroffenen gemäß § 24 DSG 2000 sowohl auf der Homepage der Liftanlagenbetreiber, als auch in den allgemeinen Geschäftsbedingungen sowie - mittels Piktogrammen - direkt beim Zugang zur Liftanlage. Das Datenverarbeitungsregister stellt für diese Datenanwendung in DVR-Online ein entsprechend adaptiertes Ausfüllmuster zur Verfügung.

b. Das internetbasierte Hinweisgebersystem „BKMS®“ zur Aufklärung von Wirtschafts- und Korruptionsdelikten der „Zentralen Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption“ wurde nunmehr im Echtbetrieb registriert. Als ausdrückliche Rechtsgrundlage hierfür dient § 2a Abs. 6 StAG. Davor erfolgte lediglich ein Probebetrieb (vgl. dazu den Datenschutzbericht der Datenschutzbehörde aus dem Jahr 2014, Seite 19, Pkt. 3.2.5.b). Das System bietet Bürgern die Möglichkeit, in gewissen Verdachtsfällen Meldungen an die Staatsanwaltschaft zu erstatten und mit dieser zu kommunizieren.

c. Basierend auf einer bestehenden Registrierung der ÖBB-Personenverkehr AG, aufgrund derer bereits seit mehreren Jahren Videoüberwachungsanlagen in speziellen Typen von Nahverkehrszügen eingesetzt werden dürfen, wurde nunmehr auch die beantragte, typenunabhängige Erweiterung auf grundsätzlich alle Personenzüge der Auftraggeberin (unter sinngemäßer Beibehaltung der Rahmenbedingungen) registriert.

d. Die Meldung der Videoüberwachung eines Privatgrundstückes wurde für diejenigen Teile der Liegenschaft, welche die Auftraggeberin ausschließlich für Wohnzwecke nutzt, registriert. Dies jedoch unter der Auflage, dass ein Servitutsweg, welcher über einen Teil des Grundstücks der Auftraggeberin verläuft und welcher von ihrem Nachbar mitbenützt werden darf, nicht von den Kameras erfasst werden darf. Da die Auftraggeberin und der Nachbar seit Jahren miteinander im (Gerichts-)Streit liegen, bestand keine Möglichkeit, die Zustimmung des Nachbarn für die Überwachung des Weges einzuholen. Da der betreffende Servitutsweg die einzige zumutbare Möglichkeit für den Nachbarn darstellt zu seinem Grundstück zu gelangen, war diese einschränkende Auflage zu erteilen. Der Bescheid wurde beim Bundesverwaltungsgericht angefochten. Eine Entscheidung über die Bescheidbeschwerde steht noch aus.

e. Registrierung eines Online-Tools, das als Hilfestellung bei der Entscheidungsfindung zur weiteren Vorgangsweise in Zusammenhang mit medizinischen und therapeutischen Maßnahmen für Patienten bietet. Diese Datenanwendung wurde insbesondere unter der Auflage registriert, dass einem Anwender vor Inanspruchnahme der Applikation bewusst sein muss, dass es sich bei dem Ergebnis, generiert durch das Tool, um eine rein automationsunterstützte Entscheidungsfindung, ohne jegliche ärztliche Einbindung handelt. Die Datenanwendung wurde ausschließlich aus datenschutzrechtlicher Sicht - nicht aus einem medizinisch/ethischen Blickwinkel - geprüft.

f. Registrierungen von Meldungen im Zuge der ELGA-Gesundheitsdatenerfassung, welche von Auftraggebern (Gesundheitsdienstanbieter) aus den ELGA-Proberegionen Wien und Steiermark eingebracht wurden. Das Datenverarbeitungsregister stellt hierfür über DVR-ONLINE zwei mit dem Bundesministerium für Gesundheit erarbeitete Ausfüllmuster (für

öffentliche bzw. für private Gesundheitsdiensteanbieter) zur Verfügung.

g. Gemeinsam mit der Österreichischen Fußball-Bundesliga und dem Österreichischen Fußballbund wurde ein Ausfüllmuster Stadionverbotsdatei zum Zweck der Festlegung und Aussprache örtlicher Hausverbote sowie zur Beantragung von bundesweiten Stadionverboten erarbeitet.

h. Ein bereits bestehendes Ausfüllmuster Flugmedizin (EMPIC Systemsoftware) zum Zweck der Verarbeitung von Antrags- und flugmedizinischen Untersuchungsdaten von Piloten, Flugverkehrsleitern und Flugbegleitern wurde aktualisiert.

Ablehnungen:

- Ablehnung einer beabsichtigten Videoüberwachung im Vorraum einer Toilette: In einer Diskothek sollten im Vorraum der Herrentoilette unter anderem die Waschbecken, die Spiegel und der Papierkorb direkt vor den WC-Kabinen videoüberwacht werden. Die Datenschutzbehörde würde eine Videoüberwachung an einer solchen Örtlichkeit nur dann zulassen, wenn die Kamera im Innenbereich des Vorraums das Bildmaterial ausschließlich verpixelt aufzeichnet. Eine zweite „scharf“ gestellte Kamera im Außenbereich des Vorraums der WC-Anlage könnte so angebracht werden, dass man die Personen dann in weiterer Folge identifizieren kann. Da der Auftraggeber im vorliegenden Fall keine verpixelte, sondern eine herkömmliche Videoüberwachung im Vorraum einsetzen wollte, wurde die Registrierung der Meldung abgelehnt.
- Bescheidmäßige Ablehnung eines Kreditinformationssystems eines öffentlichen Auftraggebers (Fachverband) mangels ausreichender Rechtsgrundlage: Ein Fachverband wollte für seine Mitglieder ein erweitertes Bonitätsservice anbieten. Dieses Service umfasste neben zugekauften Bonitätsdaten einer bekannten Kreditauskunftei zusätzlich auch Daten aus der Führung einer Liste über (Forderungs-)Betreibungsmaßnahmen über Personen, welche in der entsprechenden Branche tätig sind. Bei Vorliegen eines rechtlichen Interesses eines Anfragenden sollte eine Auskunftserteilung an diesen ergehen. Der Auftraggeber beabsichtigte damit ein vorabkontrollpflichtiges Kreditinformationssystem durchzuführen. Für Auftraggeber des privaten Bereichs ist das Vorliegen einer Gewerbeberechtigung gemäß § 152 GewO 1994 Voraussetzung, um eine Auskunftei über Kreditverhältnisse betreiben zu dürfen. Nach Auffassung der Datenschutzbehörde mangelte es dem Auftraggeber jedoch an einer ausdrücklichen gesetzlichen Zuständigkeit oder rechtlichen Befugnis im Sinne des § 7 Abs. 1 DSG 2000. Die Rechtsgrundlage, auf die sich der Auftraggeber stützte, war zu allgemein (etwa „Unterstützung der Mitglieder“) und somit als nicht ausreichend für die Durchführung eines Kreditinformationssystems anzusehen. Insofern fehlte dem Auftraggeber die in § 6 Abs. 1 Z 1 DSG 2000 erforderliche Befugnis zur Verwendung von Daten auf rechtmäßige Weise. Der Bescheid, mit dem die Registrierung der Meldung im Datenverarbeitungsregister abgelehnt wurde, wurde vom Auftraggeber angefochten. Eine Entscheidung des Bundesverwaltungsgerichtes über die Bescheidbeschwerde stand bei Redaktionsschluss aus.

3.2.6 Stammzahlenregisterbehörde

Allgemeines

Die für das Funktionieren des bereichsspezifischen eindeutigen Identifikationssystems im österreichischen E-Government erforderlichen Datenanwendungen, nämlich das Stammzahlenregister, das Ergänzungsregister für natürliche Personen, das Ergänzungsregister für sonstige Betroffene und das Vollmachtenregister, werden von der Datenschutzbehörde als Auftraggeberin im datenschutzrechtlichen Sinn betrieben.

Stammzahlenregister

Im Jahr 2015 wurden 130 Millionen bereichsspezifische Personenkennzeichen berechnet.

Vollmachtenregister

Zwischen 2011 und 2014 wurden 1.752 Vollmachten in das Vollmachtenregister eingetragen. 2015 wurden 559 Vollmachten eingetragen. In Vertretung gehandelt wurde 14.213 Mal. Berufsmäßige Parteienvertreter haben das Service 2.666 Mal benutzt.

Ergänzungsregister für natürliche Personen

In den Jahren 2011 bis 2014 wurden über 19.000 neue Personen in das Ergänzungsregister für natürliche Personen eingetragen. 2015 wurden 105.073 neue Personen in dieses Register eingetragen. Insgesamt waren zum Stichtag 31.12.2015 135.949 Personen eingetragen.

Ergänzungsregister für sonstige Betroffene :

2014 enthielt das Register 1.354.000 aktive und 199.400 inaktive Unternehmen (125.200 Neueintragungen und 476.700 Änderungen). 2015 enthielt das Register 1.368.000 aktive und 295.000 inaktive Unternehmen (125.600 Neueintragungen und 683.000 Änderungen). 2015 wurden 5.000.000 Datensätze mit Stammzahlen ausgestattet. Das Register wurde 782.200 Mal über die Weboberfläche abgefragt und 26.177.000 Mal von Behörden über die zur Verfügung gestellte Schnittstelle durchsucht.

Die Funktionen 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 Stammzahlenregisterbehörde 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 Stammzahlenregisterbehörde – 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 Dienstleistungen bequem elektronisch abzuwickeln und schützt gleichzeitig die Betroffenen vor einer leichteren Zusammenführbarkeit ihrer Daten.

Ergänzungsregister

Die DSB betreibt in ihrer Funktion als Stammzahlenregisterbehörde zwei 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 Übertragung einer Vollmacht von einer Bürgerkarte auf eine andere. Darüber hinaus wird vom Bundesministerium für Finanzen das Unternehmensserviceportal (USP) betrieben, das Unternehmen eine ähnliche Funktionalität anbietet.

Entwicklungen

In ihrem 11jährigen Bestehen hat die Stammzahlenregisterbehörde ca. 860 Millionen bPK im Rahmen der Erst- und Folgeausstattung ausgestellt und bewältigt derzeit etwa 5,5 Millionen Abfragen monatlich über die zur Verfügung gestellten Schnittstellen. Ca. 60% dieser Anfragen konnten mit der Rückübermittlung eines bPK positiv erledigt werden. 105.073 Personen wurden in das ErNP und 125.600 in das ERsB eingetragen.

Im Berichtszeitraum wurde das Angebot von E-Government Anwendungen erweitert und die Nutzung dieses Angebots nimmt zu.

Die elektronische Gesundheitsakte (ELGA)

Die elektronische Gesundheitsakte (ELGA) wurde im Dezember 2015 erstmals mit Inhalten öffentlicher Krankenanstalten und Pflegeeinrichtungen verbunden. Damit diese Inhalte mit der Bürgerkarte abgefragt werden können, hat die Stammzahlenregisterbehörde durch Mitwirkung an zahlreichen Datenaufbereitungsmaßnahmen zur Hebung der Datenqualität und durch die Bereitstellung einer eigenen Schnittstelle zur Erfassung von ELGA - relevanten Identitäten, die nicht im ZMR gefunden werden konnten, dazu beigetragen, dass diese entweder gefunden wurden oder in das Ergänzungsregister für natürliche Personen eingetragen werden konnten. Dabei wurden große Anstrengungen unternommen, um das Risiko von Doppel- und Fehleintragungen besonders niedrig zu halten.

Bankenpaket

Am 14. August 2015 wurde das sogenannte „Bankenpaket“ im BGBl. I 2015 / 116[1] kundgemacht, mit dem ein neues Kontenregister- und Konteneinschaugesetz (KontRegG), ein Bundesgesetz über die Meldepflicht von Kapitalabflüssen und von Kapitalzuflüssen (Kapitalabfluss-MeldeG) und das Bundesgesetz zur Umsetzung des gemeinsamen Meldestandards für den automatischen Austausch von Informationen über Finanzkonten (GMSG), sowie Änderungen im Bankwesengesetz, im EU - Amtshilfegesetz und im Amtshilfe - Durchführungsgesetz beschlossen wurden.

Die Datenschutzbehörde gab im Rahmen des Begutachtungsverfahrens am 3. Juni 2015 eine Stellungnahme zum Gesetzesentwurf[2] ab. Im Wesentlichen werden im Rahmen der Umsetzung dieses Pakets alle Konten und deren Inhaber der in Österreich niedergelassenen Banken in einer Datenbank erfasst; darüber hinaus müssen bestimmte Kapitalabflüsse (Auslandsüberweisungen) und rückwirkend bestimmte Kapitalzuflüsse dem Finanzministerium von den Banken gemeldet werden. Ähnlich wie bei der Transparenzdatenbank ist vorgesehen, dass die Daten von Personen im Rahmen des Bankenpakets in der Regel mit einem bereichsspezifischen Kennzeichen verknüpft sind, mit dem im Anlassfall die Verbindung zur betroffenen Person hergestellt werden kann.

Die Datenschutzbehörde ist als Stammzahlenregisterbehörde gemeinsam mit ihren Dienstleistern durch die Pflicht zur raschen Ausstattung der Daten von Kreditinstituten und Meldepflichtigen mit bereichsspezifischen Personenkennzeichen bzw. Stammzahlen gefordert.

Um die großen Datenmengen im Rahmen der Erstausstattung und die Betreuung von mehr als 700 Erstausstattungswerbern bewältigen zu können, waren neue technische Konzepte und die Schaffung eines automationsunterstützten Geschäftsprozessablaufes notwendig.

Steuerreformgesetz 2015 / 2016 „Spenden und sonstige Beiträge im Sinne von § 18 Abs. 8 EStG

Am 14. August 2015 wurde das „Steuerreformpaket 2015/16“ im BGBl. I 2015 / 118[3] kundgemacht, mit dem unter anderem veränderte Regelungen im Einkommensteuergesetz 1988 betreffend die Berücksichtigung von Beiträgen (etwa Beiträge an Kirchen und Religionsgesellschaften) und Zuwendungen (etwa Spenden) als Sonderausgaben beschlossen wurde.

Die Datenschutzbehörde gab im Rahmen des Begutachtungsverfahrens am 3. Juni 2015 eine Stellungnahme zum Gesetzesentwurf ab.

Die Datenschutzbehörde als Stammzahlenregisterbehörde wird mit der Ausstattung der Daten von Empfängern der Beiträge und Zuwendungen gemäß § 18 Abs. 8 Ziffer 1 EStG mit verschlüsselten bereichsspezifischen Personenkennzeichen für Steuern und Abgaben in der Umsetzung gefordert sein. Die Datenschutzbehörde schätzt[4], dass es im Spendenbereich rund 4.000 bis 5.000 Spendenempfänger gibt, die jährlich etwa 5 Millionen Spenden (Zahlungen) erhalten. Damit eine Spende steuerlich mindernd wirken kann, muss für jede Spende vom Spendenempfänger der Spendenbetrag und das verschlüsselte bPK des Spenders an das Bundesministerium für Finanzen übermittelt werden.

1 https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2015_I_116/BGBLA_2015_I_116.pdf
2 Stellungnahme DSB siehe https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03953/imfname_421959.pdf
3 https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2015_I_118/BGBLA_2015_I_118.pdf
4 Die Schätzung wurde der Stellungnahme der DSB zum Gesetzesentwurf „Steuerreformpaket 2015/2016 entnommen.

3.2.7 Amtswegige Prüfverfahren

Die DSB hat im Jahr 2015 67 amtswegige Verfahren nach § 30 DSG 2000 eingeleitet; 97 amtswegige Verfahren wurden im Berichtszeitraum abgeschlossen.

Ausgewählte Verfahren:

D213.336 bis D213.339

Diese Prüfverfahren dienten der Umsetzung des ersten Prüfungsschwerpunktes der Datenschutzbehörde. Die Datenschutzbehörde prüft jährlich in Schwerpunktverfahren Auftraggeber bestimmter Sektoren im Hinblick auf die Einhaltung datenschutzrechtlicher Bestimmungen.

Das erste Schwerpunktverfahren betreffend Kreditauskunfteien wurde 2014 eingeleitet und 2015 abgeschlossen.

Das Verfahren ergab, dass die untersuchten Kreditauskunfteien die Einhaltung datenschutzrechtlicher Bestimmungen gewährleisten, konkrete Empfehlungen waren keine auszusprechen.

D213.356

In diesem Verfahren untersuchte die Datenschutzbehörde, ob der von einer Schulbehörde organisierte Eignungstest von Schülerinnen und Schülern für den Arbeitsmarkt datenschutzkonform gestaltet war. Die Schulbehörde konnte dies nachweisen, das Verfahren wurde eingestellt.

D213.393

Dieses Prüfverfahren wurde über Ersuchen einer deutschen Finanzbehörde eingeleitet und betraf den „International Common Law Court of Justice“, eine Einrichtung, die sich an nationale Rechtsvorschriften nicht gebunden fühlt. Gegenstand des Verfahrens war die namensbezogene Veröffentlichung bestimmter Mitarbeiter eines deutschen Finanzamtes, gegen die eine „Klage“ beim International Common Law Court of Justice“ eingereicht worden war. Auch wenn der International Common Law Court of Justice zu erkennen gab, sich nicht an Entscheidungen der Datenschutzbehörde gebunden zu erachten, wurden die Namen der betroffenen Mitarbeiter dennoch entfernt, weshalb das Verfahren einzustellen war.

D213.395 bis D213.399

Diese Verfahren dienen der Umsetzung des Prüfungsschwerpunktes 2015 im Krankenanstaltenbereich. Die Datenschutzbehörde prüft dabei bei insgesamt fünf öffentlichen Krankenanstaltenträgern, ob datenschutzrechtliche Bestimmungen eingehalten werden. Zum Zeitpunkt der Berichtslegung sind die Verfahren anhängig.

D213.403

Dieses Prüfverfahren (zum Berichtszeitpunkt noch nicht abgeschlossen) behandelt die Datenverwendung 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.

3.2.8 Äußerungen in Beschwerdeverfahren vor dem Bundesverwaltungsgericht

Das Bundesverwaltungsgericht hat im Jahr 2014 seine Tätigkeit aufgenommen, und im Berichtszeitraum waren die Verfahren beim Bundesverwaltungsgericht bereits Routine für die Datenschutzbehörde.

Es gab im Berichtszeitraum zwei Säumnisbeschwerden, wobei die Verfahren formlos eingestellt werden konnten, weil die Bescheide nachgeholt wurden (§ 16 Abs. 1 2. Satz Verwaltungsgerichtsverfahrensgesetz (VwGVG), BGBl. I Nr. 33/2013 idgF. In einem Fall wurde der Bescheid vor Einlangen der Säumnisbeschwerde erlassen.

Es gab im Berichtszeitraum 29 Beschwerden gegen Bescheide der Datenschutzbehörde. Die überwiegende Anzahl betraf Bescheide in Beschwerdeverfahren gemäß § 31 DSG 2000, aber es gab auch Beschwerden gegen andere Entscheidungen, wie Internationaler Datenverkehr oder Bescheide in Registrierungsverfahren.

Einige ausgewählte Entscheidungen folgen an dieser Stelle. Weitere sind auf der Seite des Bundesverwaltungsgerichts im Rechtsinformationssystem des Bundes (RIS) veröffentlicht.

Beschwerde gegen den Bescheid D178.591/0001-DSB/2015 (offen)

Die Datenschutzbehörde hatte einen Antrag auf Genehmigung zur Überlassung von Daten einer Inkassofirma an mehrere andere Inkassounternehmen im Ausland abgelehnt, weil diese Empfänger, die im Ausland genauso wie die Beschwerdeführerin im Inland Forderungen betreiben, deren rechtlichen Status teilen und ebenfalls Auftraggeber sind. Der Antrag hätte daher auf Übermittlung, nicht Überlassung lauten müssen.

Entscheidung W214 2011104-1 vom 30.01.2015

Das Bundesverwaltungsgericht bestätigte die ablehnende Haltung der Datenschutzbehörde zu „Dashcams“, Videokameras im Auto, die Videos der Umgebung als Beweismittel bei Verkehrsunfällen aufnehmen sollen. Die rechtliche Befugnis zum Betrieb einer Dashcam wurde verneint. Die Revision an den Verwaltungsgerichtshof wurde zugelassen, weil es sich um eine Rechtsfrage handelt, die weit über den Einzelfall hinaus von Bedeutung ist. Revision an den Verwaltungsgerichtshof wurde erhoben, das Verfahren ist offen.

Entscheidung W214 2014733-1 vom 20.10.2015

Wenn ein Auskunftsbegehren einer Konzerntochter mit dem Vermerk „ergeht in Kopie an“ gleichzeitig der Konzernmutter übersendet wird, ist die Konzernmutter erkennbar nicht Adressat und muss das Begehren nicht auf sich beziehen. Die Pflicht zur Auskunftserteilung trifft in diesem Fall außschließlich die Konzerntochter. Das Bundesverwaltungsgericht hat die Rechtsansicht der Datenschutzbehörde bestätigt.

Entscheidung W214 2114281-1 vom 17.11.2015

Die Beschwerdeführerin verlangte ua., dass die Datenschutzbehörde für sie eine Feststellungsklage gemäß § 32 Abs. 5 DSG 2000 erheben soll. Das Bundesverwaltungsgericht wies die Beschwerde ab und bestätigte die Rechtsansicht der Datenschutzbehörde, dass kein subjektiv-öffentlicher Anspruch auf Klageerhebung durch die Datenschutzbehörde besteht.

3.2.9. Stellungnahmen zu Gesetzes- und Verordnungsvorhaben

Die DSB hat im Jahr 2015 zu folgenden Gesetzes- und Verordnungsvorhaben eine Stellungnahme abgegeben:

– Zentralverwahrer-Vollzugsgesetz – ZvVG

– Einlagensicherungs- und Anlegerentschädigungsgesetz– ESAEG

– Informationsweiterverwendungsgesetz 2005 –IWG 2005

– Meldepflicht-Änderungsgesetz

– Änderung des Staatsanwaltschaftsgesetzes

– Änderung des Börsegesetzes 1989, des Kapitalmarktgesetzes und des Rechnungslegungs-Kontrollgesetzes

– Meldepflicht-Änderungsgesetz

– Polizeiliches Staatsschutzgesetz, Änderung des Sicherheitspolizeigesetzes

– Änderung des Investmentfondsgesetzes 2011 und des Immobilien-Investmentfondsgesetzes

– Bankenpaket

– Sozialbetrugsbekämpfungsgesetz und Änderung von Begleitgesetzen

– Schulrechtsnovelle (Datenverbund)

– Steuerreformgesetz 2015/2016

– Wissenschaftsfonds-Novelle 2015

– Änderung des Telekommunikationsgesetzes, des KommAustria-Gesetz u.a.

– Gerichtsgebühren-Novelle 2015

– Informationsfreiheitsgesetz

4 Wesentliche höchstgerichtliche Entscheidungen

4.1 Beschwerden vor dem Verfassungsgerichtshof

Im Jahr 2015 hatte sich der Verfassungsgerichtshof (VfGH) im unmittelbaren Vergleich mit dem Vorjahr (siehe Datenschutzbericht 2014, 27 ff) seltener mit Fragen des Datenschutzrechts zu befassen.

Im Jahr 2015 ist keine Beschwerde gemäß Artikel 144 B-VG wegen Eingriffs in verfassungsgesetzlich gewährleistete Rechte oder Anwendung eines verfassungswidrigen Gesetzes gegen einen vom Bundesverwaltungsgericht (BVwG) bestätigten Bescheid der DSB vom VfGH inhaltlich abschließend behandelt worden.

In drei Fällen hat der VfGH von seinem Recht gemäß Artikel 144 Abs. 2 B-VG Gebrauch gemacht, die inhaltliche Behandlung eingebrachter Beschwerden mangels Aussicht auf Erfolg oder mangels Relevanz in verfassungsrechtlicher Hinsicht durch Beschluss abzulehnen.

Alle drei Verfahren (Beschlüsse vom 11.3.2015, E1143/2014, E1144/2014 und E1145/2014) betrafen vor allem die Frage des Rechtsschutzes nach Ablehnung der physischen Vernichtung („Löschung“) von Papierakten (hier konkret: Akten kriminalpolizeilicher Ermittlungsverfahren). Diese langjährige rechtliche Streitfrage ist vom VfGH bereits im Erkenntnis vom 10.12.2014, B1187/2013 (Datenschutzbericht 2014, 28 f), dahingehend geklärt worden, dass der Datenschutzbehörde ganz allgemein keine Zuständigkeit zukommt, über die Vernichtung von Papierakten zu entscheiden.

§ 83 Abs. 1 des Verfassungsgerichtshofgesetzes 1953 (VfGG) ist in Folge Aufhebung durch das Erkenntnis des VfGH vom 29.11.2014, G 30/2014 u. a. (Datenschutzbericht 2014, 27), mit Wirkung vom 1. Juli 2015 ersatzlos außer Kraft getreten. In verfassungsgerichtlichen Verfahren, die Bescheide der DSB zum Gegenstand haben, ist demnach nicht mehr kraft ausdrücklicher gesetzlicher Anordnung die DSB Beschwerdegegner. Die Verteidigung von Erkenntnissen eines Verwaltungsgerichts vor dem VfGH obliegt nun (gemäß den Erwägungen des VfGH im zitierten Erkenntnis) in erster Linie dem Gericht. Im einzigen im Jahr 2015 nach Außerkrafttreten der Bestimmung anhängig gemachten VfGH-Verfahren (E2424/2015, EU-Agrarmarktförderungen und Transparenzdatenbank), das einen Bescheid der DSB zum Gegenstand hat, ist die DSB als mitbeteiligte Amtspartei behandelt worden.

4.2. Europäischer Gerichtshof

4.2.1 Weltimmo

- Das Datenschutzrecht eines Mitgliedstaates kann auf eine ausländische Gesellschaft angewendet werden, die in diesem Staat mittels einer festen Einrichtung eine tatsächliche und effektive Tätigkeit ausübt[5].

5 Eine sehr gute Zusammenfassung bietet die Pressemitteilung Nr. 115/15 des EuGH, abrufbar unter http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150111de.pdf

Mit Urteil vom 1.10.2015 hat der Europäische Gerichtshof in der Rechtssache C-230/14 Weltimmo s.r.o. / Nemzeti Adatvédelmi és Információszabadság Hatóság (Nationale ungarische Behörde für Datenschutz und Informationsfreiheit) im Rahmen eines Vorabentscheidungsersuchens der Kúria (Oberster Gerichtshof, Ungarn) entschieden, Art. 4 Abs. 1 Buchst. a[6] der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 sei dahingehend auszulegen, dass er die Anwendung des Datenschutzrechts eines anderen Mitgliedstaats zulässt (als dem, in dem der für die Datenverarbeitung Verantwortliche eingetragen ist), soweit der Verantwortliche mittels einer festen Einrichtung im Hoheitsgebiet dieses Mitgliedstaats eine effektive und tatsächliche Tätigkeit ausübt, in deren Rahmen diese Verarbeitung ausgeführt wird, selbst wenn die Tätigkeit nur geringfügig ist.

Hinsichtlich der Prüfung, ob eine effektive und tatsächliche Tätigkeit des für die Datenverarbeitung Verantwortlichen vorliegt führt der EuGH im Ausgangsverfahren „Weltimmo" als berücksichtigungswürdig an:

- das Betreiben von Websites, die (in diesem Fall) der Vermittlung von Immobilien im Hoheitsgebiet des Mitgliedstaates dienen, in dessen Sprache verfasst sind, sowie hauptsächlich oder gar vollständig auf den Mitgliedsstaat ausgerichtet sind; sowie des weiteren,
- das Vorhandensein eines Vertreters des für die Datenverarbeitung Verantwortlichen in diesem Mitgliedstaat, der dafür zuständig ist, die Forderungen aus dieser Tätigkeit einzuziehen sowie den Verantwortlichen im Verwaltungsverfahren und im gerichtlichen Verfahren über die Verarbeitung der betreffenden Daten zu vertreten[7];

Gleichzeitig spricht der Europäische Gerichtshof[8] aus, dass - soweit die mit Beschwerden befasste Kontrollstelle eines Mitgliedstaats nach Art. 28 Abs. 4 der Richtlinie 95/46 zum Schluss gelangt, dass das auf die Verarbeitung der betreffenden personenbezogenen Daten anwendbare Recht nicht das Recht dieses Mitgliedstaats ist (sondern das eines anderen Mitgliedstaats), die Art. 28 Abs. 1, 3 und 6 dieser Richtlinie dahin auszulegen seien, dass diese Kontrollstelle die wirksamen Einwirkungsbefugnisse, die ihr gemäß Art. 28 Abs. 3 dieser Richtlinie übertragen sind, nur im Hoheitsgebiet ihres Mitgliedstaats ausüben und keine Sanktionen auf der Grundlage des Rechts dieses Mitgliedstaats gegen den für die Verarbeitung dieser Daten Verantwortlichen verhängen darf, der nicht im Hoheitsgebiet dieses Mitgliedstaats niedergelassen ist. In solch einem Fall muss sie nach Art. 28 Abs. 6 die Kontrollstelle jenes Mitgliedstaates, dessen Recht anwendbar ist, ersuchen, einzuschreiten.

4.2.2 Safe Harbor

- Der Gerichtshof erklärt die Entscheidung der Kommission, in der festgestellt wird, dass die Vereinigten Staaten von Amerika ein angemessenes Schutzniveau übermittelter personenbezogener Daten gewährleisten, für ungültig[9].

Mit Urteil vom 06.10.2015 hat der Europäische Gerichtshof in der Rechtssache C-362/14 Maximilian Schrems / Data Protection Commissioner Ireland im Rahmen eines Vorabentschei-

6 Artikel 4 Abs 1 lit a der RL 95/46/EG regelt die Anwendung des einzelstaatlichen Rechts auf alle personenbezogene Datenverarbeitungen, die im Rahmen einer Niederlassung des für die Datenverarbeitung Verantwortlichen im betreffenden Mitgliedsstaat durchgeführt werden.

7 Darüberhinaus hatte Weltimmo s.r.o. in Ungarn ein Bankkonto für den Forderungseinzug und ein Postfach zur laufenden Abwicklung der Geschäfte;

8 Siehe RZ 56 ff. des EuGH Erkenntnis unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=701747

9 Eine sehr gute Zusammenfassung bietet die Pressemitteilung Nr. 117/15 des EuGH, abrufbar unter http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117de.pdf

dungsersuchens des High Court Ireland entschieden, Art. 25 Abs. 6[10] der Richtlinie 95/46/EG sei im Licht der Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union[11] dahin auszulegen, dass eine aufgrund dieser Bestimmung ergangene Entscheidung wie die Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000[12] über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes (…) eine Kontrollstelle eines Mitgliedstaats im Sinne von Art. 28 der Richtlinie in geänderter Fassung nicht daran hindert, die Eingabe einer Person zu prüfen, die sich auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung sie betreffender personenbezogener Daten, die aus einem Mitgliedstaat in dieses Drittland übermittelt wurden, bezieht, wenn diese Person geltend macht, dass das Recht und die Praxis dieses Landes kein angemessenes Schutzniveau gewährleisteten.

Gleichzeitig hat der Europäische Gerichtshof unter Spruchpunkt 2. erkannt, dass die Entscheidung 2000/520 ungültig[13] ist.

Auszug aus dem Urteil (RZ 64,65):

Falls die Kontrollstelle zu dem Ergebnis kommt, dass das Vorbringen, auf das sich eine solche Eingabe stützt, unbegründet ist, und die Eingabe deshalb zurückweist, muss der Person, von der die Eingabe stammt, nach Art. 28 Abs. 3 Unterabs. 2 der Richtlinie 95/46 im Licht von Art. 47 der Charta der Rechtsweg offenstehen, damit sie eine solche sie beschwerende Entscheidung vor den nationalen Gerichten anfechten kann. Angesichts der in den Rn. 61 und 62 des vorliegenden Urteils angeführten Rechtsprechung müssen diese Gerichte das Verfahren aussetzen und dem Gerichtshof ein Ersuchen um Vorabentscheidung über die Gültigkeit vorlegen, wenn sie der Auffassung sind, dass einer oder mehrere der von den Parteien vorgebrachten oder gegebenenfalls von Amts wegen geprüften Ungültigkeitsgründe durchgreifen (vgl. in diesem Sinne Urteil T & L Sugars und Sidul Açúcares/Kommission, C-456/13 P, EU:C:2015:284, Rn. 48 und die dort angeführte Rechtsprechung).

Hält die Kontrollstelle die Rügen der Person, die sich mit einer Eingabe zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten an sie gewandt hat, dagegen für begründet, muss sie nach Art. 28 Abs. 3 Unterabs. 1 dritter Gedankenstrich der Richt-

10 Art. 25 Abs. 6 der RL 95/46 EU regelt, dass die Kommission nach dem Verfahren des Artikels 31 Absatz 2 der RL 95/46/EG feststellen kann, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

11 Artikel 7 „Achtung des Privat- und Familienlebens", Artikel 8 „Schutz personenbezogener Daten", Artikel 47 „Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht" der Charta der Grundrechte der EU;

12 ENTSCHEIDUNG DER KOMMISSION vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA" abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32000D0520&from=de

13 In RZ 90 des Urteils nimmt der Europäische Gerichtshof darauf Bezug, dass seine Analyse der Entscheidung 2000/520 durch die von der Kommission selbst vorgenommene Beurteilung der aus der Umsetzung dieser Entscheidung resultierenden Sachlage bestätigt wird. Insbesondere in den Abschnitten 2 und 3.2 der Mitteilung COM(2013) 846 final sowie in den Abschnitten 7.1, 7.2 und 8 der Mitteilung COM(2013) 847 final, stelle die Kommission fest, dass die amerikanischen Behörden auf die aus den Mitgliedstaaten in die Vereinigten Staaten übermittelten personenbezogenen Daten zugreifen würden und sie in einer Weise verarbeiten, die namentlich mit den Zielsetzungen ihrer Übermittlung unvereinbar sei und über das hinausgehe, was zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig sei.

linie 95/46 im Licht insbesondere von Art. 8 Abs. 3 der Charta ein Klagerecht haben. Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen.

5. Internationale Zusammenarbeit

5.1 Europäische Union

5.1.1. Die Art. 29 Datenschutzgruppe

Die aus den Vertretern der nationalen Datenschutz-Kontrollstellen (iSd Art. 28 der RL 95/46) und einem Vertreter der Europäischen Kommission zusammengesetzte Art. 29 Datenschutzgruppe hat sich im Berichtszeitraum insbesondere mit folgenden Themen auseinander gesetzt (sämtliche Dokumente sind auf Englisch verfügbar und auf der Website der Art. 29 Gruppe abrufbar):

a) Update of Opinion 8/2010 on "Applicable law in light of the CJEU judgement in Google Spain" (WP 179)

b) Guidelines for Member States on "The criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes (WP 234)

c) Opinion 03/2015 on "The draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data" (WP 233)

d) Statement on "The implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)"

e) Opinion 02/2015 on "C-SIG Code of Conduct on Cloud Computing" (WP 232)

f) Opinion 01/2015 on "Privacy and Data Protection Issues relating to the Utilisation of Drones" (WP 231)

g) Explanatory Document on "The Processor Binding Corporate Rules" (WP 204)

h) Statement of the WP29 on "Automatic inter-state exchanges of personal data for tax purposes" (WP230)

i) "Cookie sweep combined analysis" (WP229)

Sämtliche zitierten Arbeitspapiere können auf der Website der EU-Kommission unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm nachgelesen werden. Des Weiteren ist auf die zahlreichen, ebenfalls auf der oben genannten Website unter http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/index_en.htm abrufbaren, Pressemitteilungen der Art. 29 Datenschutzgruppe hinzuweisen.

Hinsichtlich der zukünftigen Entwicklung der Art. 29 Datenschutzgruppe ist anzumerken, dass diese mit dem Inkrafttreten der EU-Datenschutzgrundverordnung durch den einzuführenden

Europäischen Datenschutzausschuss abgelöst wird. Der europäische Datenschutzausschuss wird im Rahmen des in Kapitel VII der EU-Datenschutzgrundverordnung geregelten Kohärenzverfahrens auch für alle Mitgliedstaaten bzw. deren Datenschutzbehörden bindende Beschlüsse fassen können, die vor dem EuGH bekämpft werden können.

5.1.2 Europol

Europol verarbeitet große Mengen von vor allem strafrechtsrelevanten Daten. Diese Verarbeitung unterliegt der besonderen Kontrolle durch eine gemeinsame Kontrollinstanz, die aus Vertretern aller EU Datenschutzbehörden besteht, dem „Europol Joint Supervisory Body" (JSB) auf Grundlage des Art. 34 des Europol Beschlusses[14]. 2015 wurden von der Kontrollinstanz neben der jährlichen allgemeinen Überprüfung von Europol, die rechtliche Stellung von Opfern von Menschenhandel und deren oft gleichzeitige Behandlung als Täter in den Datenbanken der Strafverfolgungsbehörden, das Terrorist Finance Tracking Programme (TFTP) der Vereinigten Staaten, die Europol Plattform für Datenschutzexperten im Bereich der Strafverfolgung (Europol Data Protection Experts Network – EDEN), die Verarbeitung von Daten insbesondere im Rahmen internationaler Zusammenarbeit im Zuge der Terrorismusbekämpfung, und der Erstellung einer Webseite mit Fahndungsausschreibungen aus allen EU Mitgliedsstaaten untersucht. Begleitend analysiert wurde der legislative Prozess zur Erarbeitung eines neues Rechtsrahmens für Europol (Europol Verordnung). Ihre förmliche Annahme nach der Einigung des Rates mit dem europäischen Parlament über eine Kompromissfassung am 4.12.2015 wird im Laufe des Jahres 2016 erwartet

5.1.3 Schengen

Das Schengener Informationssystem ist ein System zur Suche bzw. Fahndung nach Personen und Sachen, das von Grenz-, Zoll-, Visa- und Strafverfolgungsbehörden genutzt wird. Das zentrale von der EU als Auftraggeber geführte SIS II wird von den nationalen Gegenstücken (N.SIS II) eingesehen und befüllt. Das N.SIS II wird in Österreich vom Bundesministerium für Inneres als Auftraggeber betrieben. Auf der Webseite der DSB ist ein Formular (mit englischer Übersetzung) für die Auskunft aus dem SIS II abrufbar. Die SIS II Verordnung[15] sieht eine koordinierte Aufsicht durch die nationalen Datenschutzbehörden mit dem Europäischen Datenschutzbeauftragten vor und eine individuelle Prüfung der N.SIS Datenverarbeitungsvorgänge alle 4 Jahre.

Mitarbeiter der Datenschutzbehörde haben als nationale Experten an den Evaluierungen aufgrund der Verordnung (EU) Nr. 1053/2013 des Rates vom 7. Oktober 2013 zur Einführung eines Evaluierungs- und Überwachungsmechanismus für die Überprüfung der Anwendung des Schengen-Besitzstands[16] in Deutschland und dem Königreich der Niederlande mitgewirkt.

5.1.4 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)[17] ein-

14 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:de:PDF
15 VERORDNUNG (EG) Nr. 1987/2006 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)
16 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32013R1053
17 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=URISERV:l33046

gerichtet wurde. Untersucht wurde von der Kontrollinstanz neben der jährlichen allgemeinen Überprüfung die Verwendung von personenbezogenen Daten im Europäischen Amt für Betrugsbekämpfung (OLAF).

5.1.5 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[18] sieht eine koordinierte Aufsicht und jährliche stichprobenartige Prüfung durch die nationale Datenschutzbehörde und die anderen EU Datenschutzbehörden mit dem Europäischen Datenschutzbeauftragten vor.

5.1.6 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[19]. 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 die österreichische Vertretungsbehörde im Vereinigten Königreich geprüft.

5.1.7 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 1. bis 3. Juli 2015 die 32. Plenarsitzung des T-PD in Straßburg statt. Die Tagesordnung sowie der zusammenfassende Bericht der Sitzung sind in englischer Sprache unter http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/OJ_T-PD32(2015)_En%20(11%2006%202015).asp abrufbar.

18 http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32013R0603
19 http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32008R0767