dsb

Republik Österreich

Datenschutz behörde

Datenschutzbericht 2014

Datenschutzbericht 2014

Wien, 2015

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, 2015

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 und löste in dieser Funktion – unter Übernahme aller Aufgaben – die Datenschutzkommission ab. Zu diesen Aufgaben zählt die Führung von Individualverfahren auf Antrag, aber auch des Datenverarbeitungs- und des Stammzahlenregisters. Zudem überprüft die DSB von Amts wegen und ist als aktives Mitglied in zahlreichen internationalen und nationalen Gremien präsent.

Die Behörde wurde im Laufe des Jahres 2014 neu strukturiert, Arbeitsfelder gestrafft und ein gemeinsames Verständnis der Mitarbeiterinnen und Mitarbeiter von der Arbeit in den unterschiedlichen Bereichen entwickelt. Durch Bündelung der Ressourcen und das außergewöhnliche Engagement von Mitarbeiterinnen und Mitarbeitern ist es gelungen, einen Großteil des Rückstandes im Datenverarbeitungs- sowie im Stammzahlenregister zu bearbeiten und abzuschließen, ohne andere Arbeitsfelder der Behörde zu vernachlässigen.

Der Datenschutzbericht 2014 ist der erste, gemäß § 37 Abs. 5 DSG 2000, nunmehr 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.

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) mit Bescheid zu genehmigen.

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

Die zahlenmäßig umfangreichste Aufgabe der Datenschutzbehörde besteht in der Erteilung von Rechtsauskünften an Bürger. Die Datenschutzbehörde erteilt jedoch nur insoweit Rechtsauskünfte, 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, ein Hinweisgeber- 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 Laienrichter,

§ 39 DSG 2000). Urteile 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 die Führung des Ergänzungsregisters und die Errechnung von Stammzahlen.

Die Datenschutzbehörde ist 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 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 25 Personen in Teil- oder Vollzeit ihren Dienst bei der Datenschutzbehörde, davon 12 Juristinnen und Juristen, 4 Mitarbeiterinnen im gehobenen Dienst und 9 Mitarbeiterinnen und Mitarbeiter im Fachdienst. Die Bediensteten der Datenschutzbehörde sind in Erfüllung ihrer Aufgaben nur an die Weisungen der Leitung gebunden.

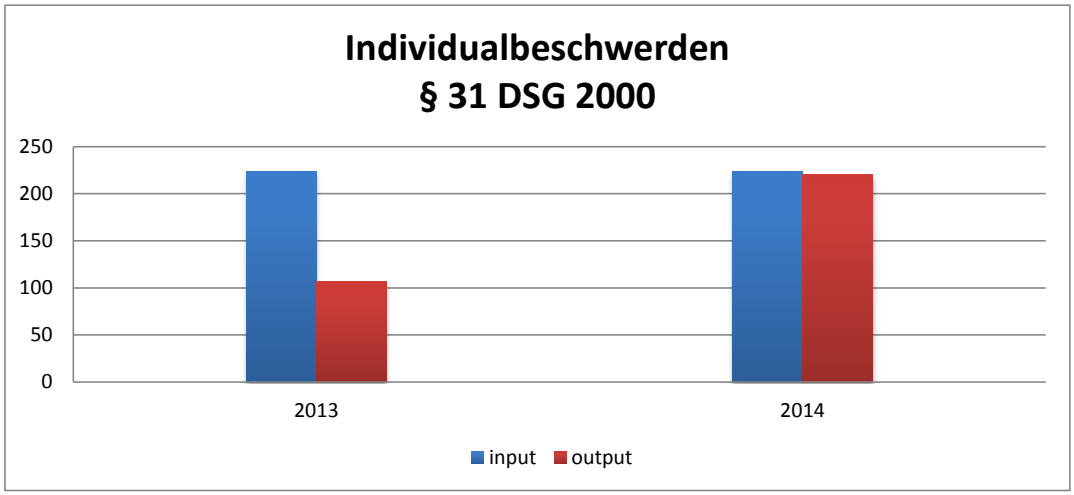
Erfreulicherweise ist es gelungen, den Personalstand im Jahr 2014 durch interne Umschichtungen und unter Nutzung der mobilitätsfördernden Maßnahmen für Mitarbeiterinnen und Mitarbeiter im Bundesdienst geringfügig zu erhöhen. Diese Maßnahmen waren jedenfalls erforderlich, da durch Personal- und Diensthoheit der Behörde Aufgaben zufallen.

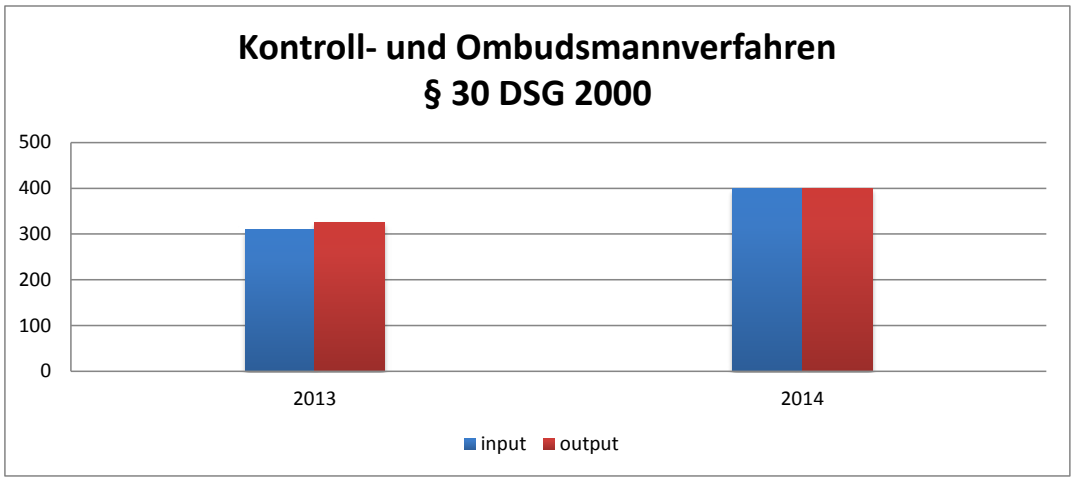
3 Tätigkeit der Datenschutzbehörde

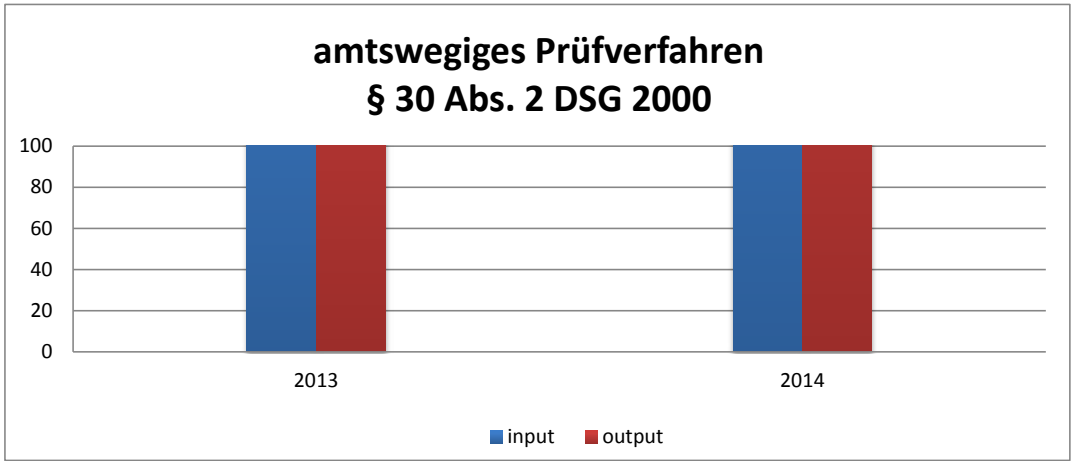
3.1 Statistische Darstellung

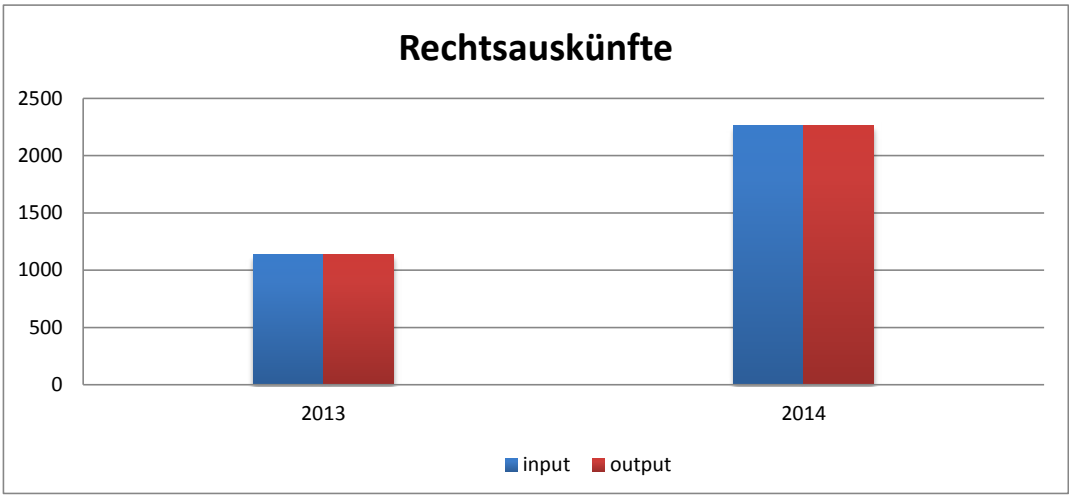
Tabelle 1 Anzahl der EIngangsstücke und Erledigungen, jeweils in den Jahren 2013 und 2014

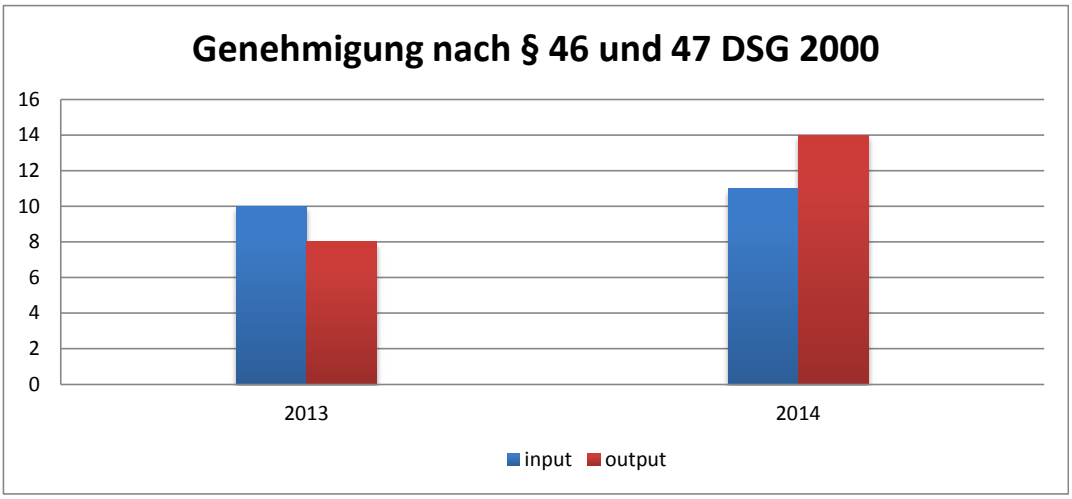
	Eingangsstücke		Erledigungen	
Art der Tätigkeit	**2013**	**2014**	**2013**	**2014**
Individualbeschwerden	224	224	107	220
Erledigungsart der Individualbeschwerden	224	224	73 Bescheide 34 Einstellungen	117 Bescheide 103 Einstellungen
Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (Verfahren über Antrag)	309	399	326	400
Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (amtswegiges Prüfverfahren)	79	98	80	88
Rechtsauskünfte	1133	2261	1133	2261
Genehmigungen nach § 46 und 47 DSG 2000 (wissenschaftliche Forschung u Statistik)	10	11	8	14
Genehmigungen im Internationalen Datenverkehr	48	79	41	80
Auskunft Schengen	42	33	39	33

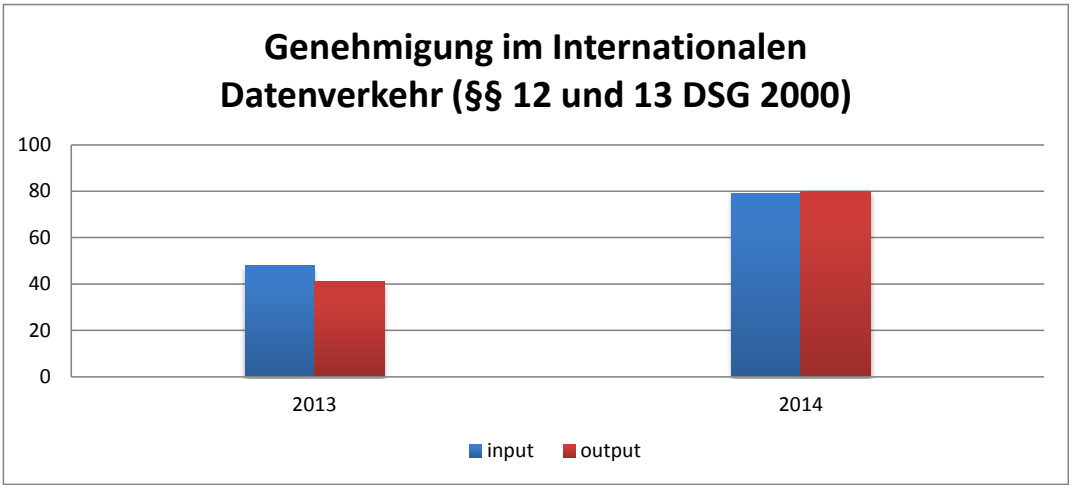


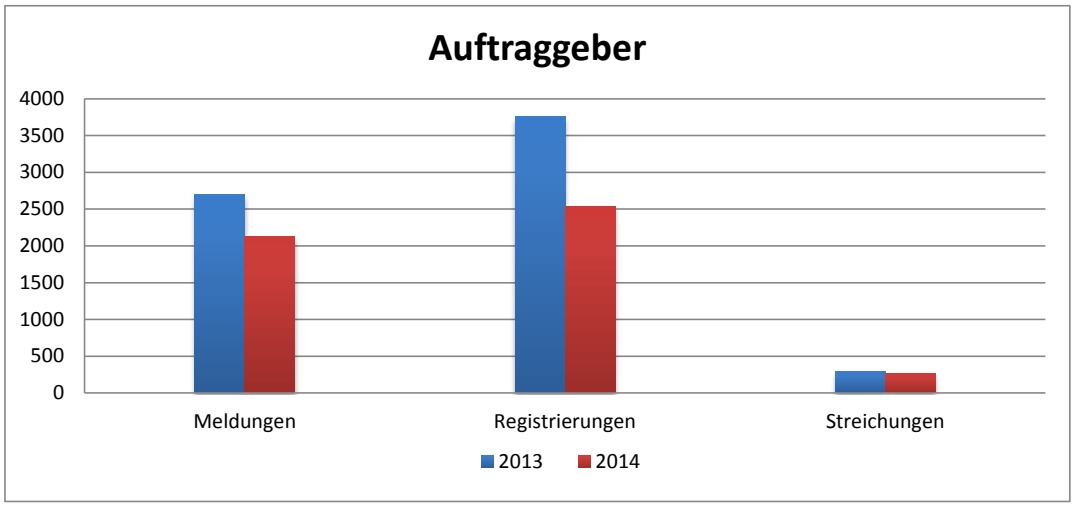












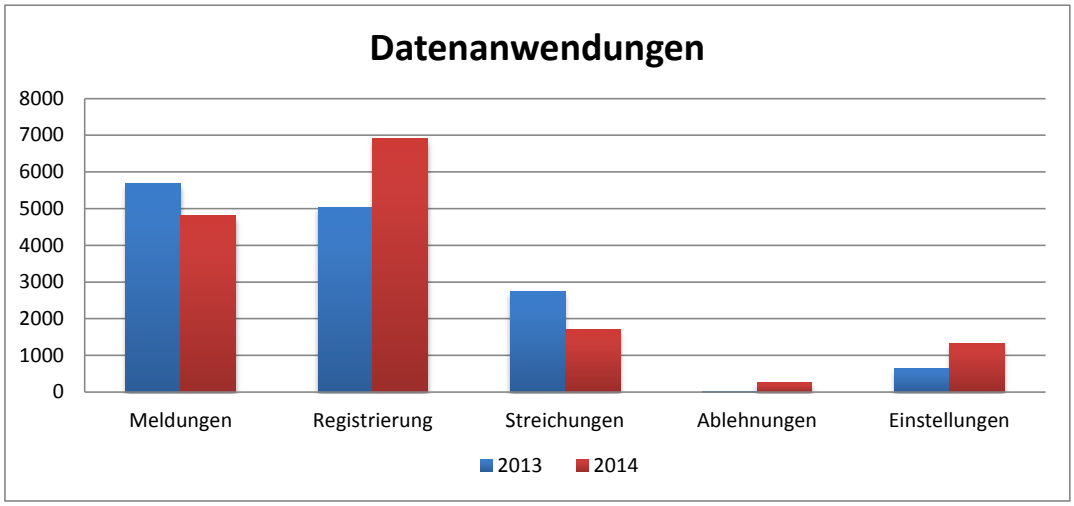


Tabelle 2 Anzahl der Tätigkeiten betreffend Datenverarbeitungsregister in den Jahren 2013 und 2014

Tätigkeiten	2013	2014
Tätigkeiten für Auftraggeber in Summe	**7012**	**4918**
Meldungen	2698	2125
Registrierungen	3752	2533
Streichungen	292	260
Tätigkeiten in Datenanwendungen in Summe	**14088**	**15039**
Meldungen	5681	4802
davon automatisch registriert	ca. 26 %	ca. 48%
Registrierungen	5040	6917
Streichungen	2733	1712
Ablehnungen	4	263
Einstellungen	630	1331
Ablehnungsbescheid	0	6
Auflagenbescheid	0	2
Richtigstellung des Registers	0	6
Verbesserungsaufträge in Summe	**1261**	**1175**

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. Solche 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 gegenüber einer Verwaltungsbehörde geltend gemacht, so entscheidet diese durch einen nicht in Form eines Bescheids ergehenden Verwaltungsakt („Mitteilung"), der nicht von den Verwaltungsgerichten, sondern von der Datenschutzbehörde zu überprüfen ist. 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 2014

Erfahrungsgemäß machen sich in den Medien präsente Themen (wie in den Jahren vor 2014 die Debatte um die Vorratsdatenspeicherung) oder bekannt gewordene Missstände bzw. „Da-

tenschutzskandale“ 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 Datenschutzbehörde – ist fokussiert auf das Ermittlungsverfahren zur Feststellung des für die Entscheidung wesentlichen Sachverhalts. Aus dem ersten Jahr der Beobachtung ist noch kein fester Trend abzuleiten, doch deuten einzelne Entscheidungen der Rechtsmittelinstanzen (etwa der Beschluss des BVwG vom 10.9.2014, W214 2008456-1) darauf hin, dass dem Ermittlungsverfahren noch höherer Aufwand zu widmen sein wird.

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 2014 als wesentlich für die Arbeit der Datenschutzbehörde erwiesen. Sie ermöglicht es, insbesondere 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 2014 konnten 103 Verfahren durch Einstellung beendet werden.

Ausgewählte Beschwerdeentscheidungen aus 2014

Die Datenschutzbehörde hat in ihrer öffentlich zugänglichen Entscheidungsdokumentation (im Rahmen des Rechtsinformationssystems des Bundes – RIS; Stand: Ende Februar 2015) für 2014 fünfzehn Bescheide aus Beschwerdeverfahren dokumentiert. Vier davon sind Ersatzbescheide, die die Rechtsprechung der Datenschutzkommission (nach Aufhebungen durch den Verwaltungsgerichtshof – VwGH wegen Unzuständigkeit, siehe VwGH Erkenntnis vom 24.4.2013, 2011/17/0156) wiederholen und bekräftigen.

Durch die Etablierung des Bundesverwaltungsgerichts als Rechtsmittelinstanz gegen die Entscheidungen der Datenschutzbehörde, ist die Bedeutung der Rechtsprechung der Datenschutzbehörde für die verbindliche Auslegung und Weiterentwicklung des Datenschutzrechts reduziert, aus diesem Grund ist die Anzahl der im RIS dokumentierten Entscheidungen verringert worden. Bis auf einen Fall (siehe unten) sind ausschließlich rechtskräftige Entscheidungen dokumentiert.

Die wichtigsten Beschwerdeentscheidungen in chronologischer Reihenfolge:

a) Bescheid vom 24.1.2014, DSB-K121.998/0001-DSB/2014

In dieser Sache hat die Datenschutzbehörde frühere Entscheidungen der Datenschutzkommission bekräftigt, wonach die Landesregierung (und nicht die Bezirksverwaltungsbehörde als Strafbehörde oder die Landespolizeidirektion als ausführende Einheit) bei automatischer Verkehrsüberwachung (hier: Abstands- und Geschwindigkeitsmessung) auf einer Autobahn als Auftraggeber die datenschutzrechtliche Verantwortung trägt.

b) Bescheid vom 5.5.2014, DSB-D122.010/0011-DSB/2014

In einem arbeitsgerichtlichen Prozess um das Dienstverhältnis einer Bediensteten einer Anstalt öffentlichen Rechts wurden Daten vom Dienst-PC der Betroffenen vom Dienstgeber dazu verwendet, den Beweis von Pflichtenverletzungen zu erbringen. Die Datenschutzbehörde sah die Übermittlung der Daten – nicht alle Behauptungen der Beschwerdeführerin waren nachweisbar – als denkmöglich beweisrelevant und nicht überschießend, daher als zulässig an.

c) Bescheid vom 14.7.2014, DSB-D121.726/0001-DSB/2014

In diesem, nach Aufhebung eines Bescheids der Datenschutzkommission durch den Verfassungsgerichtshof – VfGH ergangenen, Ersatzbescheid hat die Datenschutzbehörde nach Aufhebung von § 140 Abs. 3 StPO (VfSlg 19801/2013) entschieden, dass eine „Zweitverwertung" des Ergebnisses einer gesetzmäßig angeordneten Rufdaten- und Standortdatenrückerfassung aus einem strafprozessualen Ermittlungsverfahren im Disziplinarverfahren gegen einen Beamten durch keine gesetzliche Ermächtigung gedeckt war und das Recht des Betroffenen auf Geheimhaltung verletzt hat.

d) Bescheid vom 5.9.2014, DSB-D122.126/0007-DSB/2014

Der Beschwerdeführer brachte vor, durch den Aufdruck seines Geburtsdatums und die Angabe des Gegenstands des Zustellstücks bei der Zustellung einer Anonymverfügung (§ 49a VStG) im Recht auf Geheimhaltung verletzt worden zu sein. Die Datenschutzbehörde hat dieser Beschwerde gegen die Verwaltungsstrafbehörde Folge gegeben. Anders als Strafverfügungen und Straferkenntnisse enthalte eine Anonymverfügung keinen direkten (verwaltungs-) strafrechtlichen Vorwurf gegen den Adressaten. Daher sei auch die Beifügung des Geburtsdatums zwecks verwechslungsfreier Zustellung nicht erforderlich und damit nicht zulässig. Dieser Bescheid erwuchs in Rechtskraft; ein inhaltlich gleichlautender Bescheid wurde vor dem Bundesverwaltungsgericht bekämpft. Das Verfahren ist offen.

e) Bescheid vom 5.9.2014, DSB-D122.105/0015-DSB/2014

In dieser Sache kam die Datenschutzbehörde zu dem Schluss, dass hier zwar die Verwendung von Meldedaten zur Versendung von Einladungen (Diskussionsveranstaltungen) durch ein Organ einer Gebietskörperschaft (Bezirksvorsteher eines Wiener Gemeindebezirks) gesetzlich gedeckt war, nicht jedoch die anschließende Rückmeldung von Zustellanständen (möglicherweise unrichtig gewordenen Meldeadressen) an die Meldebehörde (Amtshilfe ohne entsprechendes Ersuchen).

f) Bescheid vom 1.10.2014, DSB-D122.020/0012-DSB/2014

Dieser Bescheid ist nicht rechtskräftig und im Berichtszeitpunkt Gegenstand eines offenen Rechtsmittelverfahrens vor dem BVwG. Im Zuge der Diskussion um die Vorratsdatenspeicherung (VDS) wurde eine Reihe von Auskunftsverlangen von Betroffenen an VDS-pflichtige Unternehmen gerichtet. In allen der Datenschutzbehörde bekannt gewordenen Fällen wurde dabei eine Auskunftserteilung über den Inhalt gespeicherter Vorratsdaten von den Auftraggebern abgelehnt. In mehreren solchen Fällen wurde Beschwerde erhoben. Nach Aufhebung der Bestimmungen über die VDS durch den Verfassungsgerichtshof (VfGH Erkenntnis vom 27.6.2014, G 47/2012 u. a., Kundmachung BGBl. I Nr. 44/2014) erhielt der Beschwerdeführer hier die – sachverhaltsmäßig unbestrittene – Auskunft, dass die über ihn gespeicherten Vorratsdaten gelöscht wurden. Der Beschwerdeführer bestritt nun die Rechtmäßigkeit der Löschung (wegen § 26 Abs. 7 DSG 2000) und begehrte die Feststellung, durch die Verweigerung der Auskunft bis zum Zeitpunkt der Löschung im Recht auf Auskunft verletzt gewesen zu sein. Die Datenschutzbehörde hat dies mit der tragenden Begründung abgewiesen, das Beschwerdeverfahren diene der Durchsetzung des Rechts auf Auskunft und nicht der Feststellung möglicher vergangener Rechtsverletzungen. „Ein durch eingetretene faktische Unmöglichkeit nicht mehr durchsetzbares Recht kann gemäß § 31 Abs. 7 und 8 DSG 2000 auch nicht zum Gegenstand der Feststellung gemacht werden, in diesem Recht in der Vergangenheit verletzt gewesen zu sein."

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 (einem Anbringen) 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 nach § 30 Abs. 6 DSG 200 ist die Herbeiführung des rechtmäßigen Zustands. Dazu kann die DSB auch – nicht durchsetzbare – Empfehlungen aussprechen. Zumeist wird im Rahmen eines solchen Verfahrens eine datenschutzrechtlich zufriedenstellende Situation ohne Einsatz dieses Mittels erreicht.

Hervorzuheben ist in diesem Zusammenhang, dass als Folge des Urteils des Europäischen Gerichtshofes (EuGH) vom 13. Mai 2014 (Rechtssache C 131/12), wonach der Betreiber einer Suchmaschine unter bestimmten Umständen Verweise (Hyperlinks) auf personenbezogene Daten aus seinem Index streichen muss, im Berichtszeitraum 11 diesbezügliche Fälle im Rahmen des Kontroll- und Ombudsmannverfahrens an die DSB herangetragen wurden.

Die zahlenmäßig größte Gruppe von Eingaben betraf, wie in den Vorjahren, Fragen der Videoüberwachung. 2014 waren dies 159 Kontroll- und Ombudsmannverfahren zu dieser Thematik. Darüber hinaus wurden 62 amtswegige Verfahren zu Videoüberwachungen geführt.

Im Berichtszeitraum scheinen folgende Fälle besonders erwähnenswert:

a) Empfehlung betreffend die Meldung an den Jugendwohlfahrtsträger aufgrund des Verdachts auf Vernachlässigung, Misshandlung, Quälen oder sexuellen Missbrauch (DSB-K215.309/0001-DSB/2014, 29. Jänner 2014)

Bei der Einschreiterin wurde in einem Landeskrankenhaus ein Wadenbeinbruch diagnostiziert. Die Traumaanamnese der knöchernen Veränderung an beiden Unterschenkeln der Einschreiterin war nicht möglich, zudem ergab sich ein Hinweis auf eine ältere Fraktur und fiel als Zufallsbefund ein posttraumatisches Knochenmarksödem an der linken Tibia auf. Nachdem die Mutter der Einschreiterin zur Verletzungsursache und zu den Lebensumständen und dem sozialen Umfeld der Einschreiterin befragt und dokumentiert wurde, dass sich die Mutter nicht überlastet fühlte und eine liebevolle Mutter-Kind-Aktion stattfand, erstattete die Krankenanstaltsträgerin eine Gefährdungsmeldung an die zuständige Jugendwohlfahrtsbehörde.

Die DSB erkannte in ihrer Entscheidung im Gegensatz dazu eindeutige Indizien, die gegen den Verdacht einer Gewaltanwendung bzw. einer Vernachlässigung der Einschreiterin sprachen. Dabei betonte sie, dass das Vorliegen eines hinreichend konkreten Verdachts conditio sine qua non für die Rechtmäßigkeit einer Übermittlung auf Basis des § 54 ÄrzteG sei. Nur wenn ein derartiger Verdacht bestehe, der sich auch durch zumutbare Ermittlungsmaßnahmen (wie etwa Befragungen etc.) nicht entkräften lässt, sei daher die Übermittlung personenbezogener Daten durch § 7 Abs. 2 iVm §§ 8 und 9 DSG 2000 gedeckt und stellt somit einen zulässigen Eingriff in das Grundrecht auf Datenschutz dar. Welche Ermittlungsmaßnahmen zumutbar seien, sei einzelfallbezogen zu beurteilen, wobei bei einer (öffentlichen) Krankenanstalt jedoch, da diese über einen entsprechenden administrativen Hilfsapparat bzw. über ärztliches Wissen verschiedener Fachrichtungen verfüge, ein strenger Maßstab anzulegen sein werde.

Die DSB empfahl, der Krankenanstaltenträger möge durch geeignete Maßnahmen sicherstellen, dass eine Meldung an den Jugendwohlfahrtsträger lediglich im Falle eines hinreichend konkreten Verdachts auf Vernachlässigung, Misshandlung, Quälen oder sexuellen Missbrauchs erfolge.

b) Empfehlung betreffend die Verwendung der Sozialversicherungsnummer zur Erstellung eines Benutzer-Accounts (DSB-D213.131/0002-DSB/2014, 23. Mai 2014)

Die Errichtung eines persönlichen Zuganges zu einem System im medizinischen Bereich erforderte die Aufnahme der Stammdaten des betreffenden medizinischen Personals einschließlich der Sozialversicherungsnummer in das Personalverwaltungssystem des Auftraggebers. Dabei diente die Heranziehung der Sozialversicherungsnummer der Nutzer der Identifizierung und Authentifizierung bei der Einrichtung eines persönlichen Accounts, durch diese Maßnahme sollte sichergestellt werden, dass es sich um eine echte Person handelt.

Unter Verweis auf die Rechtsprechung der ehemaligen Datenschutzkommission (vgl. die Empfehlung vom 19. Juli 2013, GZ K210.741/0016-DSK/2013), wonach die Sozialversicherungsnummer nicht als „genereller Identifikator“ verwendet werden dürfe, verneinte die DSB hier einen sozialversicherungsrechtlichen Zusammenhang, weil die Verwendung der Sozialversicherungsnummer nur der Identifizierung und Authentifizierung eines potentiellen Nutzers zur Erlangung einer Zugangsberechtigung zu einem System diene. Darüber hinaus war im Lichte des sich aus § 1 Abs. 2 letzter Satz und § 7 Abs.3 DSG 2000 ergebenden Grundsatzes für die Datenschutzbehörde nicht nachvollziehbar, weshalb den gesetzlichen Anforderungen der §§ 3 bis 5 Gesundheitstelematikgesetz 2012 in Verbindung mit dem E Government-Gesetz, nur unter Zuhilfenahme der Sozialversicherungsnummer entsprochen werden könnten, zumal lediglich festgestellt werden sollte, ob es sich beim potentiellen Nutzer um eine „echte Person“ handle. Bei einem behandelnden Arzt könnte die Klärung dieser Frage etwa auch unter Verwendung der Ärzteausweisnummer oder überhaupt – im Einklang mit dem E-Government-Gesetz – mittels Bürgerkarte erfolgen.

Folglich wurde die Empfehlung ausgesprochen, das hier zuständige Amt der Landesregierung möge von der Verwendung der Sozialversicherungsnummer bei Erstellung eines näher bezeichneten Benutzer-Accounts absehen.

c) Empfehlung zur Verwendung von Wählerdaten aus dem Wählerverzeichnis hinsichtlich einer vom Bürgermeister selbst finanzierten Befragung der Gemeindebürger zum geplanten Flüchtlings- und Asylwerberheim (DSB-D215.548/0007-DSB/2014, 28. November 2014)

Ein Bürgermeister verwendete zum Zweck der Aussendung eines Schreibens betreffend eine selbstfinanzierte Volksbefragung Daten aus dem Wählerverzeichnis der Gemeinde.

Die DSB ging sowohl auf Grund des gegenständlichen Schreibens als auch der eigenen Angaben des Bürgermeisters davon aus, dass dieser in seiner amtlichen Funktion als Bürgermeister in Erscheinung getreten sei. Als Organ einer Gebietskörperschaft (Gemeinde) bedürfe er daher für die Verwendung personenbezogener Daten, unabhängig ob automationsunterstützt oder nicht, gemäß § 1 Abs. 2 DSG 2000 einer (formal)gesetzlichen Grundlage (siehe dazu auch den Bescheid der Datenschutzkommission vom 25. April 2012, GZ K121.760/0016-DSK/2012). Angelegenheiten des Asylwesens seien gesetzlich nicht dem eigenen Wirkungsbereich der Gemeinden zugeordnet. Die gesetzlichen Voraussetzungen zur Durchführung einer Volksbefragung nach § 61 Tiroler Gemeindeordnung 2001 – TGO, die einen Zugriff auf Daten des Wählerverzeichnisses ermöglicht hätten, seien demnach – wie auch vom Bürgermeister selbst

angegeben – nicht vorgelegen, weshalb sich die Verwendung personenbezogener Daten aus dem Wählerverzeichnis als unzulässig erwiesen habe.

Die DSB empfahl, der Bürgermeister möge von der Verwendung von Daten aus dem Wählerverzeichnis Abstand nehmen, wenn die Voraussetzungen für eine Volksbefragung nach § 61 TGO nicht vorliegen.

d) Mandatsbescheid: Keine Videoüberwachung von Mietern (DSB-D215.463/0006- DSB/2014, 22. August 2014)

Eine als Hausverwaltung bestellte GmbH suchte nach Beweisen, um einen Mietvertrag (Altbau in einem Innenstadtbezirk von Wien) kündigen zu können. Sie nahm an, der Mieter würde die Wohnung gar nicht benützen oder habe sie vertragswidrig weitervermietet, was der Mieter jedoch bestritt. Es kam zu einem Kündigungsstreit vor Gericht, woraufhin die Hausverwaltung ein Detektivunternehmen mit der Beschaffung von Beweisen beauftragte. Der Detektiv installierte eine versteckte Kamera mit digitaler Bildaufzeichnung (Auslösung durch einen Bewegungsmelder) vor der Wohnungstür, die Aufnahmen von allen Personen anfertigte, die die Wohnung betraten oder verließen.

Der Mieter wandte sich hierauf an die DSB, welche der Hausverwaltung und der Hauseigentümerin im Rahmen des Kontroll- und Ombudsmannverfahrens schließlich die Weiterführung der (nicht gemeldeten) Videoüberwachung des gegenständlichen Eingangsbereichs der Wohnung mittels Bescheid untersagte.

Die DSB hat hier zum ersten Mal einen solchen Mandatsbescheid gemäß § 30 Abs. 6a DSG 2000 erlassen, weil sie auf Grund des schwerwiegenden Eingriffs in die Privatsphäre des Mieters sowie der Möglichkeit, dass die Videobilder zum Nachteil des Mieters verwendet werden, annahm, dass „Gefahr im Verzug“ gegeben sei. Zudem betonte sie, dass eine derartige Videoüberwachung nicht dem Gesetz entspreche. Nach einem Rechtsmittel der Auftraggeber wurde der Bescheid aufgehoben, da die Anlage inzwischen bereits entfernt worden war.

3.2.3 Rechtsauskünfte an Bürgerinnen und Bürger

Die Datenschutzbehörde stellt auf ihrer Homepage umfassende Rechtsinformationen in Zusammenhang mit dem Datenschutzgesetz 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 werden auf Grund der gesetzlichen Zuständigkeit der Datenschutzbehörde im Zuge eines konkreten Verfahrens vorgenommen. Jede sonstige „Vorabbeurteilung“ würde das Ergebnis eines allfälligen Verfahrens vor der Datenschutzbehörde vorwegnehmen.

3.2.4 Genehmigungen im Internationalen Datenverkehr

Im Berichtszeitraum stand durch interne Ressourcensteuerung mehr Personal zur Bearbeitung von Anträgen zur Genehmigung für den internationalen Datenverkehr zur Verfügung. Aus diesem Grund konnten im Jahr 2014 80 Akten in diesem Bereich abgeschlossen werden.

Die Anträge kamen ausschließlich von Konzernunternehmen in Österreich, die personenbezogene Daten an Empfänger im Ausland weiter zu geben beabsichtigten. Dabei handelte es sich um Übermittlungen von Personaldaten an die Konzernzentralen und Überlassungen an

Dienstleister. Die Art der Anträge blieb unverändert; bei den rechtlichen Instrumenten zur Wahrung der schutzwürdigen Geheimhaltungsinteressen der Betroffenen war ein neuer Trend zu beobachten. Bisher wurden immer vertragliche Vereinbarungen auf Grundlage der Standardvertragsklauseln der Europäischen Union verwendet. Die parallel dazu bestehende Option, verbindliche unternehmensinterne Vorschriften (Binding Corporate Rules, kurz BCR) einzusetzen, wurde bislang kaum genutzt. Im Jahr 2013 gab es die ersten beiden Entscheidungen auf der Grundlage von BCRs, und 2014 folgten etliche weitere.

Die Binding Corporate Rules ermöglichen Datentransfers innerhalb eines Konzerns, ohne dass jedes Mal eine vertragliche Vereinbarung abgeschlossen werden muss. Die BCRs sind aufwändig bei der Erstellung, während ein Vertragsabschluss sich in der Regel einfacher gestaltet. Aus diesem Grund wurden BCRs von den Konzernen bisher nur selten eingesetzt.

Im Jahr 2014 hat die Datenschutzbehörde eine Entscheidung auf Grundlage von § 13 Abs. 4 DSG 2000 gefällt (Bescheid D178.612/0002-DSB/2014 vom 5. September 2014). Gemäß § 13 Abs. 4 DSG 2000 kann ein inländischer Dienstleister die Genehmigung zur Überlassung beantragen, wenn er zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber mehreren Auftraggebern jeweils einen bestimmten weiteren Dienstleister im Ausland heranziehen will.

3.2.5 Entscheidungen im Registrierungsverfahren

Registrierungen

a) Registriert wurde das seitens mehrerer Skiliftbetreiber-Gesellschaften gemeldete „Photocompare"-System, das der manuell-visuellen Kontrolle von Skiliftkartenbesitzern an ausgewählten Einstiegsstellen mit Hilfe des Einsatzes von Kameras dient. Zweck ist das Verhindern bzw. die Verfolgung von Liftkarten-Missbrauch. Die Datenverwendung basiert – bei bestehender Alternativmöglichkeit für Personen, die nicht an „Photocompare" teilnehmen wollen – auf einer im Zuge des Liftkartenerwerbs abgegebenen Zustimmungserklärung.

b) Das internetbasierte Hinweisgebersystem „BKMS®" zur Aufklärung von Wirtschafts- und Korruptionsdelikten, welches bei der „Zentralen Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption" eingerichtet ist, wurde im befristeten Probebetrieb registriert. Das System soll die Möglichkeit bieten, in gewissen Verdachtsfällen Meldungen an die Behörde zu erstatten und mit dieser zu kommunizieren. Beides auf Wunsch auch anonym.

c) Registrierungen im Zuge einer Apotheken-Kundendatenerfassung, welche dem Zweck dient, die bestmögliche Beratung von Kunden (vor allem in den Bereichen Selbstmedikation, Gesundheits- und Ernährungsfragen) zu garantieren und die Durchführung von Vorsorgemaßnahmen sowie deren Überwachung zu ermöglichen. Das Datenverarbeitungsregister stellt hierfür über DVR-ONLINE ein entsprechendes Ausfüllmuster zur Verfügung.

d) Die Meldung der Videoüberwachung eines Freizeitunternehmens (u.a.) im Garderobenbereich (Kästchen- bzw. Spindbereich) wurde unter der Bedingung registriert, dass die Aufnahmen dort so grob verpixelt erfolgen, dass Personen, die sich in diesem Bereich aufhalten, nur schemenhaft erkennbar sind. Der Auftraggeber argumentierte, dass gerade bei den Kästchen und Spinden die meisten Einbruchsdiebstähle stattfinden. In Kombination mit hochauflösenden Kameras außerhalb der Garderobe (bei den Ein- bzw. Ausgängen) könnte im Anlassfall dann die Bewegung des mutmaßlichen Täters innerhalb der Garderobe solange nachvollzogen werden, bis die verdächtige Person den Garderobenbereich verlässt, und eine Identifikation zur Täterausforschung stattfinden kann.

e) Die Datenschutzbehörde hat im Berichtszeitraum ein Verfahren zur effizienten Registrierung von Whistleblower-Systemen (Hinweisgebersystemen) entwickelt. Dazu wird die Regelung in § 19 Abs. 2 DSG 2000 herangezogen, wonach ein Auftraggeber zusagen kann, dass er beim Betrieb einer Datenanwendung bestimmte Auflagen oder Bedingungen beachten wird. Auf der Grundlage der bisherigen 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. Auf diese Weise wurden etliche Meldungen von Auftraggebern (meistens Konzernunternehmen) registriert.

Ablehnungen

a) Ein IT-Dienstleistungs- und Handelsunternehmen hat eine Meldung bezüglich einer Kundenkarte, die mittels automationsunterstützter Gesichtserkennung (Speicherung biometrischer Daten) Kunden beim Betreten des Geschäftes identifiziert, erstattet. Aufgrund der Bestimmung des § 50a Abs. 7 DSG 2000, welche einen solchen automatisierten Bildabgleich ausdrücklich untersagt, wurde die Registrierung diese Meldung abgelehnt.

b) Abgelehnt wurde in mehreren Fällen die mit der Absicht zur Weiterleitung von Bildmaterial an Behörden oder an Gerichte betriebene private Überwachung mittels Kameras aus dem eigenen Kfz heraus. Zweck ist die Beweismittelsicherung im Anlassfall (meistens in Folge eines Unfalles, aber darüber hinaus auch im Falle einer Sachbeschädigung oder im Falle eines Einbruches in das parkende Kfz). Für den Betrieb dieser sogenannten „Dashcams“ bzw. „Crashcams“ und der damit einhergehenden Überwachung öffentlicher Straßen und Plätze fehlt einem privaten Auftraggeber regelmäßig die hierfür erforderliche „gesetzliche Zuständigkeit“ bzw. „rechtlichen Befugnis“ im Sinne des § 7 Abs. 1 DSG 2000). Die Rechtsansicht der Datenschutzbehörde wurde vom Bundesverwaltungsgericht bestätigt.

c) Ein einzelner Wohnungseigentümer eines Mehrparteienhauses wollte in der Tiefgarage – abgesehen von seinem eigenen Parkplatz – auch den Nachbarparkplatz und das Einfahrtstor videoüberwachen. Da ein einzelner Wohnungseigentümer keine ausreichende Verfügungsbefugnis über die (für alle Bewohner) allgemein zugänglichen Räumlichkeiten eines Mehrparteienhauses (wie etwa auch Stiegenhäuser, Gänge, Gemeinschaftsgärten, Höfe) hat, musste die Registrierung der Meldung abgelehnt werden.

d) Der Inhaber eines Juweliergeschäftes wollte seine Videokameras so ausrichten, dass er bis zu einen Meter (gemessen von den Schaufenstern) auch den öffentlichen Gehsteig vor seinem Geschäft videoüberwachen hätte können. Nach ständiger Entscheidungspraxis der Datenschutzbehörde sind zu diesem Zweck maximal ca. 50 cm – von der Fassade aus gerechnet – zulässig. Dies ist der Bereich, der seitens der Datenschutzbehörde als gerade noch notwendig zur Zweckerreichung (Eigentumsschutz, Sicherung von Beweismitteln zur Ausforschung von Tätern) anerkannt wird. Da in diesem Fall zu viel öffentlicher Raum von den Kameras erfasst worden wäre, wurde die Registrierung der Meldung abgelehnt.

e) In zwei Fällen wurden Videoüberwachungen in Unternehmen abgelehnt, da der jeweilige Auftraggeber keine Betriebsvereinbarung über die Verwendung von personenbezogenen (Bild-)Daten im Zusammenhang mit den auf dem Betriebsgelände installierten Videokameras dem Datenverarbeitungsregister übermittelt hat, dies obwohl in beiden Fällen ein Betriebsrat existierte. Die Vorlage entsprechender Betriebsvereinbarungen im Registrierungsverfahren ist gemäß § 50c Abs. 1 letzter Satz DSG 2000 vorgesehen. Videoüberwachungen in Betrieben werden von der Datenschutzbehörde als System zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die

Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen, qualifiziert (vgl. § 96a ArbVG).

3.2.6 Stammzahlenregisterbehörde

Allgemeines
Die für das Funktionieren des bereichsspezifischen eindeutigen Identifikationssystems im österreichischen E-Government erforderlichen Datenanwendungen (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
In den Jahren 2011, 2012 und 2013 wurden von der Stammzahlenregisterbehörde 338.716.219 (Stand 3.12.2013) bereichsspezifische Personenkennzeichen berechnet,

2014 wurden 225.519.504 berechnet.

Vollmachtenregister
In den Jahren 2011, 2012 und 2013 wurden 1056 (Stand 3.12.2013) Vollmachten in das Vollmachtenregister eingetragen. 2014 wurden 696 Vollmachten eingetragen.

Ergänzungsregister für natürliche Personen
In den Jahren 2011, 2012 und 2013 wurden über 12.000 (Stand 30.5.2013) neue Personen in das Ergänzungsregister für natürliche Personen eingetragen. 2014 wurden 7333 neue Personen in dieses Register eingetragen. Insgesamt waren zum Stichtag 31.12.2014 31 545 Personen eingetragen.

Ergänzungsregister für sonstige Betroffene :
Für 2013 existiert keine Referenzzahl, das Register wurde neu befüllt und in Betrieb genommen. 2014 enthält das Register 1.354.000 aktive und 199.400 inaktive Unternehmen (125.200 Neueintragungen und 476.700 Änderungen). 4.500.000 Datensätze wurden mit Stammzahlen ausgestattet. Das Register wurde 475.000 mal über die Weboberfläche abgefragt und 16.500.000 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 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 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 10-jährigen Bestehen hat die Stammzahlenregisterbehörde ca. 800 Millionen bPK ausgestellt und bewältigt derzeit etwa 2 Millionen Abfragen monatlich. Ca. 60% dieser Anfragen konnten mit der Rückübermittlung eines bPK positiv erledigt werden. 40.000 Personen wurden in das ErNP und 1,3 Millionen in das ERsB eingetragen.

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

Transparenzportal und elektronische Rechnungseinbringung an die öffentliche Verwaltung

Die E-Government-Großprojekte „Transparenzportal“ und „elektronische Rechnungseinbringung“ verpflichten erstmals Förderungsnehmer oder Lieferanten des Bundes zur Nutzung der zur Verfügung gestellten E-Government Anwendungen. Insbesondere ausländische Betroffene aber auch österreichische sonstige Betroffene wie z. B. inländische kulturelle Organisationen oder Tourismusverbände mussten sich daher an die DSB wenden, um eine Eintragung in einem, mitunter aber auch in allen drei von der DSB betriebenen Register zu erwirken.

Bereichsspezifische Kennzeichen für die Verwendung im privaten Bereich

Die wichtigste Neuerung der Novelle zum E-Government-Gesetz (BGBl. I Nr. 7 / 2008) bestand darin, dass Banken und Versicherungen unter gewissen Voraussetzungen bereichsspezifische Personenkennzeichen verwenden dürfen. Dadurch wird die Qualität der Identitätsdaten der Kunden dieser Unternehmen erheblich verbessert.

Das in der vergangenen Berichtsperiode der Bundesanstalt Statistik Austria als Dienstleister zum Betrieb übergebene und mit 1,3 Millionen Unternehmen befüllte Ergänzungsregister für sonstige Betroffene (ERsB) hat seine Funktionen gut erfüllt. Die Mechanismen zur Sicherstellung der Datenqualität im Register waren gefordert, da es insbesondere im Zusammenhang mit Erstausstattungen von Datenanwendungen durch große öffentliche Auftraggeber zu zahlreichen Mehrfacherfassungen kam.

3.2.7 Amtswegige Prüfverfahren

Die DSB hat im Jahr 2014 98 amtswegige Verfahren nach § 30 DSG 2000 eingeleitet; 88 dieser Verfahren wurden im Berichtszeitraum abgeschlossen.

Ausgewählte Verfahren:

D213.262, D213.332

Dieses Prüfverfahren behandelte die Datenverwendung im Rahmen des nationalen Teils des Schengener Informationssystems II (N.SIS II) durch das Bundesministerium für Inneres. Die DSB ist aufgrund europarechtlicher Vorgaben verpflichtet, in regelmäßigen Abständen diese Datenverwendungen zu prüfen. Die Prüfverfahren ergaben keine Auffälligkeiten oder Abweichungen vom rechtmäßigen Zustand, die Verfahren konnten eingestellt werden.

D213.296

Aufgrund der medialen Berichterstattung rund um den „Datenskandal“ des Bundesinstituts für Bildungsforschung, Innovation und Entwicklung des österreichischen Schulwesens (BIFIE) leitete die DSB ein entsprechendes Prüfverfahren ein. Das Ermittlungserfahren ergab, dass seitens des BIFIE alle zumutbaren Schritte unternommen wurden, um die missbräuchliche Verwendung personenbezogener Daten zu minimieren. Das Verfahren wurde daher eingestellt.

D213.303 bis D213.305 und D213.307:

In diesen Prüfverfahren, eingeleitet aufgrund der Eingaben von vier Gemeinden, ging es um die Neugestaltung der behördlichen Gemeindeaufsicht eines Bundeslandes. Die Gemeindeaufsichtsbehörde strebte einen direkten Zugriff auf die Personaldaten der Gemeindebediensteten an, um allfällige Missstände (bspw. fehlerhafte Zulagen etc.) frühzeitig und erkennen und abzustellen. Dafür nannte die Aufsichtsbehörde verschiedene landesrechtliche Grundlagen für die Zulässigkeit des Zugriffs. Die DSB regte an, den Zugriff so zu gestalten, dass vorerst kein namentlicher Bezug zu einem bestimmten Gemeindebediensteten möglich ist und die Aufsichtsbehörde nur Einsicht in jene Daten erhalten sollte, die für aufsichtsbehördliche Zwecke erforderlich sind. Da diese Lösung technisch zu aufwändig gewesen wäre, empfahl die DSB der Landesregierung daher (Empfehlung vom 5. Dezember 2014, GZ. DSB D213.303/0015-DSB/2014), mit der Umsetzung dieses Vorhabens bis zur Schaffung einer geeigneten, diesen Zugriff legitimierenden, Rechtsgrundlage zuzuwarten.

3.2.8 Stellungnahmen der DSB in Gesetzesbegutachtungsverfahren

Die DSB hat 2014 zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Abgabenänderungsgesetz 2014
- Auslandsunterhaltsgesetz 2014
- SPG-Novelle 2014
- Hochschülerinnen- und Hochschülerschaftsgesetz 2014
- Änderung des Bundesbehindertengesetzes und des Bundessozialamtsgesetz
- Sozialversicherungs-Änderungsgesetz 2014
- Änderung des Bundes-Verfassungsgesetzes (Informationsfreiheit)
- Änderung des Ärztegesetzes 1998
- Anti-Doping-Bundesgesetz 2007
- Änderung des Eisenbahngesetzes 1957 und des Unfalluntersuchungsgesetzes
- Versicherungsaufsichtsgesetz 2016
- Änderung des Chemikaliengesetzes 1996 und des Bundeskriminalamt-Gesetzes
- 2. Abgabenänderungsgesetz 2014
- Änderung des Islamgesetzes 1912
- Änderung des Bundespflegegeldgesetzes
- Änderung Familienlastenausgleichsgesetz

Alle Stellungnahmen sind auf der Website des Parlaments (http://www.parlament.gv.at/PAKT/MESN/) abrufbar.

4 Wesentliche höchstgerichtliche Entscheidungen

4.1 Europäischer Gerichtshof (EuGH)

4.1.1 EuGH-Urteil C-293/12 und C-594/12

Der EuGH erklärt die Richtlinie zur „Vorratsdatenspeicherung von Daten“ für ungültig:

Mit Urteil vom 8.4.2014 zu C-293/12 und C-594/12 (verbundene Rechtssachen, „Digital Rights Ireland“(C-293/12) und Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl (C-594/12) hat der Europäische Gerichtshof im Rahmen eines Vorabentscheidungsersuchens des irländischen und österreichischen Verfassungsgerichtshofes die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, für ungültig erklärt.

Aus dem Urteil (Randziffer 69):

Aus der Gesamtheit der vorstehenden Erwägungen ist zu schließen, dass der Unionsgesetzgeber beim Erlass der Richtlinie 2006/24 die Grenzen überschritten hat, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta (Anmerkung: Charta der Grundrechte der Europäischen Union) einhalten musste.

Auszug aus der Pressemitteilung Nr. 54/14iii des Gerichtshofes:

Sie (Anmerkung: RL 2006/24/EG) beinhaltet einen Eingriff von großem Ausmaß und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, der sich nicht auf das absolut Notwendige beschränkt.

4.1.2 EuGH-Urteil C-212/13

Der EuGH erklärt die Datenschutzrichtlinie für eine Videoaufzeichnung eines Privaten, die (zumindest teilweise) auf öffentlichen Straßenraum gerichtet ist, für anwendbar.

Mit Urteil vom 11.12.2014 zu C-212/13 (František Ryneš/Úřad pro ochranu osobních údajů (Amt für den Schutz personenbezogener Daten)) hat der Europäische Gerichtshof im Rahmen eines Vorabentscheidungsersuchens des Nejvyšší správní soud (Oberstes Verwaltungsgericht) die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr für eine Videoaufzeichnung mit einer Überwachungskamera auf einem Einfamilienhaus, die auf den öffentlichen Straßenraum gerichtet ist, für anwendbar erklärt. Eine Überwachung mittels Videoaufzeichnung auf einer kontinuierlichen Speichervorrichtung, stellt eine automatisierte Verarbeitung personenbezogener Daten gemäß Artikel 3 Absatz 1 der Richtlinie 95/46/EG dar iv. Soweit sich die Videoüberwachung nur teilweise auf den öffentlichen Raum erstreckt (..) kann sie nicht als ausschließliche „persönliche oder familiäre“ Tätigkeit im Sinne von Art. 3 Abs. 2 der Richtlinie 95/46/EG angesehen werden.

Auszug aus der Pressemitteilung Nr. 175/14 des Gerichtshofes: Die Richtlinie ermöglicht jedoch die Würdigung des berechtigten Interesses dieser Person, das Eigentum, die Gesundheit und das Leben seiner selbst und seiner Familie zu schützen.(…).Zugleich muss das nationale Gericht bei der Anwendung der Richtlinie berücksichtigen, dass ihre Bestimmungen die Möglichkeit eröffnen, das berechtigte Interesse des für die Datenverarbeitung Verantwortlichen, das Eigentum, die Gesundheit und das Leben seiner selbst und seiner Familie zu schützen, zu würdigen.

4.1.3 EuGH-Urteil C-131/12

Der EuGH erklärt, dass der Internetsuchmaschinenbetreiber bei personenbezogenen Daten, die auf von Dritten veröffentlichten Internetseiten erscheinen, für die von ihm vorgenommene Verarbeitung verantwortlich ist („Google Sucheinträge“) und unter bestimmten Voraussetzungen eine Entfernung aus der Ergebnisliste eines Sucheintrages vorzunehmen hat:

Mit Urteil vom 13.05.2014 zu C-131/12 (Google Spain SL, Google Inc./ Agencia Española de Protección de Datos, Mario Costeja González) hat der Europäische Gerichtshof im Rahmen eines Vorabentscheidungsersuchens des Audiencia Nacional entschieden, dass Tätigkeit eines Internetsuchmaschinenbetreibers (Informationen finden, automatisch indexieren, vorübergehend speichern, Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen) als Verarbeitung personenbezogener Daten im Sinne von Art. 2 Buchstabe b der Richtlinie 95/46/EG anzusehen und der Betreiber „Verantwortlicher“ im Sinne von Art. 2 lit. d leg.cit. ist. Zur Frage der Anwendung (welches) einzelstaatlichen Rechts (Art. 4 Abs. 1 lit a RL 95/46) führt der EuGH aus, dass eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung ausgeführt wird, wenn der Suchmaschinenbetreiber in einem Mitgliedsstaat für die Förderung des Verkaufs der Werbeflächen eine Zweigniederlassung oder Tochtergesellschaft gegründet hat. Im Urteil des Gerichtshofes wird zur Auslegung von Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 festgehalten, dass der Suchmaschinenbetreiber zur Wahrung der in diesen Bestimmungen vorgesehenen Rechte , sofern deren Voraussetzungen erfüllt sind, zur Entfernung von Links auf von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person verpflichtet ist, auch dann, wenn der Name oder die Information nicht vorher oder gleichzeitig gelöscht wurden und zwar selbst dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist. Zur Prüfung der Anwendungsvoraussetzungen sind Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 dahingehend auszulegen, dass u. a. zu prüfen ist, ob die betroffene Person ein Recht darauf hat, dass die Information über sie zum gegenwärtigen Zeitpunkt nicht mehr durch eine Ergebnisliste, die im Anschluss an eine anhand ihres Namens durchgeführte Suche angezeigt wird, wobei die Feststellung eines solchen Rechts nicht voraussetzt, dass der betroffenen Person durch die Einbeziehung der betreffenden Information in die Ergebnisliste ein Schaden entsteht. Ausdrücklich hält der EuGH fest, dass in Anbetracht der Grundrechte aus den Art. 7 und 8 der Charta ein Betroffener verlangen kann, dass die betreffende Information der breiten Öffentlichkeit nicht mehr durch Einbeziehung in eine derartige Ergebnisliste zur Verfügung gestellt wird, und dass diese Rechte eines Betroffenen grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit am Zugang zu der Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche überwiegen. Dies wäre jedoch nicht der Fall, wenn sich aus besonderen Gründen – wie der Rolle der betreffenden Person im öffentlichen Leben – ergeben sollte, dass der Eingriff in die Grundrechte dieser Person durch das überwiegende Interesse der breiten Öffentlichkeit daran, über die Einbeziehung in eine derartige Ergebnisliste Zugang zu der betreffenden Information zu haben, gerechtfertigt ist.

4.1.4 EuGH-Urteil C-288/12

Der EuGH erklärt, dass die vorzeitige Beendigung des Mandats der Kontrollstelle für den Schutz personenbezogener Daten eine Vertragsverletzung gegen die Verpflichtungen aus Richtlinie 95/46EG darstellt.

Mit Urteil vom 8.4.2014 zu C-288/12 (Europäische Kommission/Ungarn) hat der Europäische Gerichtshof im Rahmen eines Vertragsverletzungsverfahrens festgestellt, dass die vorzeitige Beendigung des Mandats der Kontrollstelle für den Schutz von Personen bei der Verarbeitung personenbezogener Daten das Unabhängigkeitsgebot von Art. 28 Abs. 1 der RL 95/46/EG ver-

letzt und zwar auch dann, wenn das vorzeitige Ende des Mandats auf einer Umstrukturierung oder Änderung des Modells beruht.

4.2 Verfassungsgerichtshof

4.2.1 Allgemeines und Grundsätzliches

Im Jahr 2014 hat der Verfassungsgerichtshof für die Weiterentwicklung des Datenschutzrechts auf nationaler Ebene bedeutsame Entscheidungen getroffen.

Durch das weithin bekanntgewordene Erkenntnis vom 27.6.2014,G 47/2012 u. a., wurden die nationalen Bestimmungen über die sogenannten Vorratsdatenspeicherung (VDS) vom Verfassungsgerichtshof (VfGH) als verfassungswidrig aufgehoben.

Durch das weit weniger beachtete Erkenntnis vom 10.12.2014, B 1187/2013, hat der VfGH eine langjährige Streitfrage betreffend die „Löschung" von Daten aus Papierakten, die keine Dateien sind, geklärt. Demnach hat über die Frage, ob ein Recht auf die physische Vernichtung von Akteninhalten besteht, nicht die Datenschutzbehörde sondern die jeweils aktenführende Behörde durch Bescheid zu entscheiden.

Erwähnung finden sollte weiters das Erkenntnis vom 29.11.2014, G 30/2014 u. a., durch das § 83 Abs. 1 VfGG idF des Art. 4 des Verwaltungsgerichtsbarkeits-AusführungsG 2013 als verfassungswidrig aufgehoben worden ist. Dieses Entscheidung wird die Frage beeinflussen, ob und inwieweit die Datenschutzbehörde dazu berufen ist, bei Verfassungsbeschwerden gegen Erkenntnisse des Bundesverwaltungsgerichts (BVwG) als Beschwerdegegner vor dem VfGH aufzutreten und die Entscheidung des BVwG zu verteidigen (nach Ansicht des VfGH muss diese Rolle jedenfalls auch dem BVwG zufallen). Dem Gesetzgeber ist hier eine „Reparaturfrist" bis Ende Juni 2015 eingeräumt worden.

4.2.2 Zu den Entscheidungen im Einzelnen

VfGH Erkenntnis vom 27.6.2014,G 47/2012 u. a.

Die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt und verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (im Folgenden: VDS-RL) war ein von Beginn an rechtspolitisch sehr umstrittenes Thema. Die Diskussion um die VDS als Instrument der Sicherheitspolizei und der Strafverfolgung ist auch durch die vorliegenden höchstgerichtlichen Entscheidungen nicht beendet worden.

Der Gerichtshof der Europäischen Union (EuGH) hat (u.a. auf Grund eines Vorabentscheidungsersuchens des VfGH) mit Urteil vom 8.4.2014, C-293/12 und C-594/12 (Digital Rights Ireland Ltd, Seitlinger u. a.), ECLI:EU:C:2014:238, die VDS-RL rückwirkend für ungültig erklärt. Ein von der früheren Datenschutzkommission beim EuGH gestelltes Vorabentscheidungsersuchen (insbesondere zu Fragen der Auslegung der VDS-RL betreffend Auskunftserteilung über gespeicherte Vorratsdaten) wurde im Anschluss daran von der Datenschutzbehörde mit Schreiben an den EuGH vom 29. April 2014 zurückgezogen (EuGH Rs C-46/13).

Der VfGH hatte nun die Verfassungsmäßigkeit der nationalen Umsetzungsbestimmungen zur weggefallenen VDS-RL am Maßstab des Bundesverfassungsrechts (Art. 8 EMRK, § 1 DSG 2000) zu messen.

Der VfGH erachtete in dieser Sache die Individualanträge des Zweit- und des Drittantragstellers auf Gesetzesprüfung (Art. 140 Abs. 1 Z 1 lit c B-VG) betreffend die aufgehobenen Bestimmungen für zulässig, da „außergewöhnliche, besondere Umstände" beide davon entbinden würden, andere mögliche Rechtswege (ausdrücklich erwähnte der VfGH dabei auch ein Auskunftsbegehren gemäß § 26 DSG 2000, Erkenntnis Rz 122) zu beschreiten.

Der VfGH hielt fest, dass eine VDS wie die durch § 102a TKG 2003 angeordnete denkmöglich einen zulässigen Eingriff in die Grundrechte gemäß § 1 Abs. 1 DSG 2000 und Art. 8 EMRK bilden könnte. Es handle sich um einen „gravierenden Grundrechtseingriff" (Erkenntnis, Rz 164). Bereits die Speicherung beim Diensteanbieter sei „ein Eingriff von besonderem Gewicht" (Erkenntnis, Rz 191). Als zulässigen Zweck eines solchen Eingriffs sah der VfGH die „Bekämpfung schwerer Kriminalität" an, wobei die Zulässigkeit „von der Ausgestaltung der Bedingungen der Speicherung von Daten auf Vorrat und den Anforderungen an deren Löschung sowie von den gesetzlichen Sicherungen bei der Ausgestaltung der Möglichkeiten des behördlichen und privaten Zugriffs auf diese Daten" abhänge (Erkenntnis, Rz 164). Weiters müsse ein angemessenes Verhältnis zwischen der Schwere des konkreten Grundrechtseingriffs und der Bedeutung der mit der VDS verfolgten Ziele bestehen (Erkenntnis, Rz 166).

Die aufgehobenen Bestimmungen hätten diese Anforderungen jedoch nicht erfüllt.

Der VfGH betonte dabei die Bedeutung vertraulicher Kommunikation für die freie Persönlichkeitsentfaltung des Einzelnen in einer demokratischen Gesellschaft. Angesichts der „Streubreite" des Grundrechtseingriffs durch eine VDS (der VfGH sprach in diesem Zusammenhang wörtlich von einem „Recht auf informationelle Selbstbestimmung", Erkenntnis, Rz 168) sei die gesetzliche Grenze der Ermächtigung zur Ermittlung von Vorratsdaten durch die Behörden (Erwartung, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe bis zu einem Jahr bedroht ist, möglich wird, § 135 Abs.2a StPO) zu indifferenziert und damit zu weit gefasst. Entweder müsse die Strafdrohung höher sein, oder die Art der Tatbegehung die Verwendung von Vorratsdaten für die Aufklärung der entsprechenden Straftat „in besonderem Maße notwendig" machen. Jene Bestimmungen des SPG, die eine Verwendung von Vorratsdaten ohne diese Schranke und ohne eine richterliche Genehmigung vorsehen würden, wären in noch höherem Ausmaß unverhältnismäßig.

VfGH Erkenntnis vom 10.12.2014, B 1187/2013

In diesem Beschwerdefall hatte die frühere Datenschutzkommission eine Beschwerde wegen Verletzung des Löschungsrechts abgewiesen, weil die fraglichen Daten (zum Sexualleben der Beschwerdeführerin) nur in Form eines Aktenstücks im Papierakt eines Finanzamts vorlagen, und das Löschungsrecht gemäß § 27 Abs. 1 DSG 2000 auf solche Akten mangels Dateiqualität nicht anzuwenden ist (Bescheid vom 6.9.2013, K121.979/0014 DSK/2013).

Die dagegen erhobene Verfassungsbeschwerde (Art. 144 B-VG) machte vor allem geltend, dass die Beschwerdeführerin durch den abweisenden Bescheid in ihrem Recht auf Achtung des Privat- und Familienlebens gemäß Art. 8 EMRK verletzt worden sei.

Der VfGH bestätigte einerseits den Bescheid der Datenschutzkommission und hielt seine Rechtsprechung aufrecht, wonach ein (nicht in besonderer Weise strukturierter) Papierakt nicht dem

Löschungsrecht des DSG 2000 unterliege. Daraus folge, dass der Datenschutzbehörde auch keine Zuständigkeit zukomme, über die Vernichtung von Papierakten zu entscheiden.

Der VfGH sprach jedoch andererseits aus, dass auf Grundlage von Art. 8 EMRK und § 1 DSG 2000 der Beschwerdeführerin sehr wohl ein Recht auf Aktenvernichtung zukommen könnte: „Werden demnach Papierakten aufbewahrt, deren weitere Verwendung gegen Art. 8 EMRK verstößt, ergibt sich aus dem Recht auf Geheimhaltung ein Recht auf physische Vernichtung der Papierakten durch die Behörde. Das Finanzamt H*** hat die entsprechenden Daten daher entweder zu vernichten oder einen Bescheid zu erlassen [...]. Gegen einen abweisenden Bescheid stünde der Beschwerdeführerin der Rechtsweg an das Bundesfinanzgericht und in der Folge allenfalls an die Gerichtshöfe des öffentlichen Rechts offen."

Damit hat der VfGH faktisch ein neues, direkt und ohne einfachgesetzliche Grundlage unmittelbar aus den Verfassungsbestimmungen § 1 Abs. 1 DSG 2000 und Art. 8 EMRK ableitbares Teil-Grundrecht, das „Recht auf physische Aktenvernichtung", geschaffen, dessen Durchsetzung nicht der Datenschutzbehörde sondern den aktenführenden Behörden und den zu deren Kontrolle berufenen Verwaltungsgerichten obliegt.

4.3 Verwaltungsgerichtshof – Entscheidung zu § 50 e DSG

Der VwGH stellt klar, dass § 50e Abs. 1 DSG 2000 das Auskunftsrecht gemäß § 26 leg.cit. betreffend Videoüberwachung lediglich hinsichtlich der Form der Auskunftserteilung modifiziert.

Mit Erkenntnis vom 29.10.2014 zu Zl. 2013/01/0127 hat der Verwaltungsgerichtshof, anlässlich einer Beschwerde gegen den Bescheid der Datenschutzkommission vom 19.7.2013 betreffend der behaupteten Verletzung des Auskunftsrechtes bei einer Videoüberwachung durch ein Verkehrsunternehmen erkannt, dass ein Recht auf Auskunft nach § 50e in Verbindung mit § 26 DSG 2000 nur dann besteht, wenn das betreffende Videomaterial aufgrund eines Anlassfalles ausgewertet wurde.

Nähere Informationen befinden sich auf der Hompepage des Verwaltungsgerichtshofes unter folgendem Link:
https://www.vwgh.gv.at/aktuelles/pressemitteilungen/2014/11-2-videoueberwachung.html

5 Internationale Zusammenarbeit

5.1 Europäische Union

5.1.1 Art. 29 Gruppe

Die aus den Vertretern der nationalen Datenschutz-Kontrollstellen (iSd Art. 28 der RL 95/46/EG) und einem Vertreter der Europäischen Kommission zusammengesetzte Art. 29 Datenschutzgruppe hat sich im Jahr 2014 insbesondere mit folgenden Themen auseinander gesetzt (sämtliche Dokumente sind auf Englisch verfügbar):

a) Opinion 01/2014 on the "Application of necessity and proportionality concepts and data protection within the law enforcement sector" (WP 211)

b) Opinion 02/2014 on a "Referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents" (WP 212)

c) Opinion 03/2014 on "Personal Data Breach Notification" (WP 213)

d) Working document 01/2014 on "Draft ad hoc contractual clauses "EU data processor to non-EU sub-processor" (WP 214)

e) Opinion 04/2014 on "Surveillance of electronic communications for intelligence and national security purposes" (WP 215)

f) Opinion 05/2014 on "Anonymisation Techniques onto the web" (WP216)

g) Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" (WP217)

h) Statement on the role of a risk-based approach in data protection legal frameworks (WP218)

i) Opinion 7/2014 on the protection of personal data in Quebec (WP219)

j) Statement on the ruling of the Court of Justice of the European Union which invalidates the Data Retention Directive (WP220)

k) Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU (WP 221)

l) Statement on the results of the last JHS meeting (WP222)

m) Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223)

n) Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting (WP 224)

o) Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" (WP 225)

p) Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on “Contractual clauses” Considered as compliant with the EC Model Clauses (WP 226)

q) Joint statement of the European Data Protection Authorities assembled in the Article 29 Working Party (WP227)

r) Working Document on surveillance of electronic communications for intelligence and national security purposes (WP 228)

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

5.1.2 Europol

Bei Europol werden große Mengen personenbezogener Daten verarbeitet, die von besonderer datenschutzrechtlicher Bedeutung sind. Aus diesem Grund sind im Europol-Beschluss besondere Rechte für Betroffene vorgesehen (z. B. Art. 30 – Auskunftsanspruch; Art. 31 – Berichtigung und Löschung von Daten). Neben den nationalen Kontrollinstanzen (Art. 33) wurde eine Gemeinsame Kontrollinstanz (GKI; “Europol Joint Supervisory Body“) eingesetzt (Art. 34). Sie überprüft ob durch die Verwendung der bei Europol vorhandenen personenbezogenen Daten die Datenschutzrechte von Personen verletzt wurden und führt jährlich Inspektionen bei Europol durch. Die österreichischen Mitglieder der GKI werden von der DSB entsandt.

5.1.3 Schengen

Das (Schengener Informationssystem der 2. Generation (SIS II) ist ein Informationssystem, das Ausschreibungen zu Personen und Sachen enthält. Eine Ausschreibung ist ein in das System eingegebener Datensatz, der den zuständigen Behörden die Identifizierung einer Person im Hinblick auf die Ergreifung spezifischer Maßnahmen ermöglicht. Es wird von Grenzschutzbeamten, Zollbeamten, Visa- und Strafverfolgungsbehörden im Schengen-Raum genutzt. SIS II besteht aus einem zentralen System (dem “zentralen SIS II“), einem nationalen System („N.SIS II“) in jedem Mitgliedstaat (dem nationalen, mit dem zentralen SIS II kommunizierenden Datensystem) und einer Kommunikationsinfrastruktur zwischen dem zentralen System und den nationalen Systemen, die ein verschlüsseltes virtuelles Netz speziell für SIS-II-Daten und den Austausch von Daten zwischen den für den Austausch aller Zusatzinformationenzuständigen Behörden (SIRENE-Büros) zur Verfügung stellt.

Für das nationale System ist das Bundesministerium für Inneres (BMI) verantwortlich, das zentrale System und die Kommunikationsinfrastruktur wird von der Europäischen Kommission (inhaltlich) sowie von der neu gegründeten EU Agentur für große IT Systeme (EU-Lisa; technisch) betrieben. Die DSB ist nationale Kontrollinstanz im Sinne des Art.44 der 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-Verordnung), die das Schengener Durchführungsübereinkommen von 1990 (SDÜ) ablöst.

Es besteht eine koordinierte Aufsicht durch die nationalen Kontrollinstanzen mit dem Europäischen Datenschutzbeauftragten (EDSB). Je nach Gegenstand der Kontrolle (nationales oder zentrales System bzw. Kommunikationsinfrastruktur) ist der EDSB oder sind die nationalen Behörden zur Kontrolle berufen (vgl. Art. 46 SIS-II-Verordnung).

Das BMI trifft die Pflicht zur Auskunftserteilung gemäß §§ 1 und 26 DSG 2000 an Betroffene. Auf der Webseite der DSB ist ein Formular (mit englischer Übersetzung) für die Auskunft aus dem SIS II abrufbar.

5.1.4 Zoll

Das gemeinsame Zollinformationssystem (ZIS) der EU erlaubt es, Daten über Waren oder Transportmittel sowie über natürliche und juristische Personen zu speichern, für die es tatsächliche Anhaltspunkte gibt, dass sie im Zusammenhang mit Handlungen stehen, die der Zoll- oder der Agrarregelung zuwiderlaufen.

Das ZIS ist eine Ausschreibungsdatei im Rahmen der Betrugsbekämpfung und ermöglicht es jenem Mitgliedstaat, der die Daten in das System eingegeben hat, diese Daten einem ZIS-Partner in einem anderen Mitgliedstaat zur Durchführung gezielter Kontrollen zu übermitteln. Zur adäquaten datenschutzrechtlichen Kontrolle ist eine gemeinsame Aufsichtsbehörde (Gemeinsame Kontrollinstanz für das ZIS) eingerichtet, für die pro EU-Mitgliedsland zwei Vertreter von der jeweiligen Datenschutzbehörde nominiert werden.

5.1.5 Eurodac

Das „Eurodac"-System ermöglicht den Mitgliedstaaten, Asylbewerber und andere Personen zu identifizieren, die beim illegalen Überschreiten einer EU-Außengrenze aufgegriffen werden. Anhand des Vergleichs der Fingerabdrücke kann ein Mitgliedstaat feststellen, ob ein Fremder, der sich illegal in seinem Hoheitsgebiet aufhält, bereits 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, einer computergestützten Datenbank für Fingerabdrücke und elektronischen Einrichtungen für die Datenübertragung zwischen den Mitgliedstaaten und der zentralen Datenbank. Die von den Mitgliedstaaten übermittelten Daten umfassen auch den Herkunftsstaat, Ort und Zeitpunkt der Antragstellung, das Geschlecht sowie die Kennnummer. Namen werden in diesem System nicht gespeichert, es handelt sich daher um eine Sammlung von „indirekt personenbezogenen Daten" im Sinne des DSG 2000. Seit 2013 wird Eurodac von EU-Lisa (EU-Agengy for large-scale IT-Systems) geführt.

5.1.6 Visa

Das Visa-Informationssystem (VIS) ist ein System zum Austausch von Daten über Kurzzeit-Visa zwischen den Mitgliedstaaten des Schengenraums, das aufgrund der Entscheidung 2004/512/EG des Rates und der Verordnung (EG) Nr. 767/2008 eingerichtet wurde. Das System nahm am 11. Oktober 2011 seinen Betrieb auf. Es besteht aus einer zentralen Datenbank, einer nationalen Schnittstelle in den Schengen-Staaten und einer Infrastruktur zur Kommunikation zwischen beiden. Durch die nationalen Schnittstellen werden Daten zu allen im Schengen-Staat durchgeführten Anträgen, Ausstellungen, Ablehnungen, Annullierungen, Widerrufen und Verlängerungen von Visa durch die zuständigen Behörden in das System eingespeist.

Das VIS besteht aus einer zentralen Datenbank mit alphanumerischer Suchfunktion, und einem automatisierten System zur Identifizierung von Fingerabdrücken (AFIS), das neue und bereits in der Datenbank vorhandene Fingerabdrücke vergleicht. Der nationale Teil des VIS wird vom BMI, der zentrale Teil und die Kommunikationsinfrastruktur werden (technisch) von EU-Lisa betrieben. Die Kontrolle von VIS wird durch die nationalen Datenschutzbehörden gemeinsam mit dem EDSB ausgeübt.

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 2. bis 4. Juni 2014 die 31. Plenarsitzung des T-PD in Straßburg statt. Gegenstand der Beratungen waren u.a. die Modernisierung der Empfehlung des Ministerkomitees Nr. R (89) 2 über den Schutz personenbezogener Daten von Arbeitnehmern sowie die Modernisierung der Empfehlung des Ministerkomitees Nr. R (97) 5 über den Schutz von Gesundheitsdaten. 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-PD31(2014)_En.asp abrufbar.