# Datenschutzbericht 2018

Wien, im März 2019

**Impressum**

Medieninhaber, Herausgeber und Redaktion:
Datenschutzbehörde, Dr. Andrea Jelinek
(gemäß § 18ff DSG), Wickenburggasse 8, 1080 Wien
Kontakt: dsb@dsb.gv.at
Website: www.dsb.gv.at
*Fotonachweis:* Stefanie Korherr (Seite 6)
*Gestaltung:* Datenschutzbehörde
*Druck:* BMVRDJ
Wien, 2019

## 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 nimmt seit 25. Mai 2018 diese Aufgabe aufgrund § 18 Datenschutzgesetz (iVm Art. 51 DSGVO) wahr. Der Datenschutzbehörde obliegt seit 25.5.2018 die Führung von Individualverfahren auf Antrag, die Führung amtswegiger Verfahren, die Führung internationaler, grenzüberschreitender Verfahren, die Akkreditierung von Verhaltensregeln, die Bearbeitung von Data Breach Meldungen, die Verordnungserlassung betreffend ua. die Datenschutz-Folgenabschätzung (black list/white list) sowie die Führung von Verwaltungsstrafverfahren. Die Datenschutzbehörde ist darüber hinaus als aktives Mitglied in zahlreichen internationalen und nationalen Gremien präsent.

Die Arbeit der Datenschutzbehörde war im ersten Halbjahr 2018 - neben der täglichen Arbeit – geprägt von der Vorbereitung auf die Geltung der DSGVO ab 25. Mai 2018. Ab 25. Mai wurden die ersten Verfahren nach der DSGVO (national und international) geführt, das Datenverarbeitungsregister wurde abgewickelt und vor dem Übergang der Kompetenzen der Stammzahlenregisterbehörde auf das Bundesministerium für Digitales und Wirtschaftsstandort am 28. Dezember 2018, waren auch die Aufgaben der Stammzahlenregisterbehörde wahrzunehmen.

Die Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörde haben im Jahr 2018 sowohl national als auch international mehr als 100 Vorträge gehalten, haben unzählige Veranstaltungen besucht und haben an einem Kommentar des Datenschutzgesetzes mitgeschrieben.

Die Wichtigkeit des Grundrechts auf Datenschutz wird durch die DSGVO unterstrichen und die Aufgabe der europäischen Datenschutzbehörden ist es nunmehr, die einheitliche Anwendung der Verordnung in der europäischen Union zu gewährleisten.

An dieser Stelle sei festgehalten, dass die Datenschutzbehörde im Jahr 2018 sechs zusätzliche A1 Planstellen und zwei Planstellen für juristische Praktikanten erhalten hat. Diese Anzahl hält mit der Verdreifachung (siehe Bericht) des Beschwerdeanfalls und der zusätzlichen Tätigkeiten, die die Behörde seit 25.Mai 2018 wahrzunehmen hat, nicht mit. Aus diesem Grund wurde bereits im Jahr 2018 ein weiterer Antrag zur Personalaufstockung im A1 und A2-Bereich gestellt und ich gehe davon aus, dass die Republik Österreich die Datenschutzbehörde mit jenem Personal (Art. 52 DSGVO) ausstatten wird, damit diese ihren Verpflichtungen, die ihr aus dem DSG und der DSGVO erwachsen, nachkommen kann.

Der Datenschutzbericht 2018 ist der fünfte, gemäß § 23 Abs. 1 DSG (iVm Art. 59 DSGVO), jährlich zu erstellende Bericht über die Tätigkeit der Datenschutzbehörde, der dem Bundesminister für Verfassung, Reformen, Delegierung und Justiz 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 nationalen und internationalen Welt des Datenschutzes.

Die Datenschutzbehörde stellt einen – durchaus auch für Nicht-Juristinnen und Nicht-Juristen konzipierten – Leitfaden zur DSGVO auf ihrer Website zur Verfügung, der regelmäßig aktualisiert wird. Die jüngste Aktualisierung erfolgte im Jänner 2019

Dr. Andrea Jelinek

Leiterin der Datenschutzbehörde

# 2 Die Datenschutzbehörde

## 2.1 Organisation und Aufgaben

### 2.1.1 Die Datenschutzbehörde

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

Die Leiterin der Datenschutzbehörde ist Dr. Andrea Jelinek, der stellvertretende Leiter Dr. Matthias Schmidl. Beide wurden vom Bundespräsidenten auf Vorschlag der Bundesregierung mit 1. Jänner 2014 für die Dauer von fünf Jahren bestellt und mit Entschließung des Bundespräsidenten vom 20. Dezember 2018 für weitere fünf Jahre wiederbestellt.

### 2.1.2 Aufgaben

Bis zum Ablauf des 24. Mai 2018 nahm die Datenschutzbehörde die ihr durch das DSG 2000 übertragenen Aufgaben wahr.

Dabei handelte es sich um die Führung von

- Melde- und Registrierungsverfahren nach §§ 17 ff DSG 2000
- Verfahren betreffend internationalen Datenverkehr nach § 13 DSG 2000
- Kontroll- und Ombudsmannverfahren nach § 30 DSG 2000
- Beschwerdeverfahren nach § 31 DSG 2000,
- Verfahren betreffend die Verwendung von Daten für wissenschaftliche Forschung und Statistik nach § 46 DSG 2000 sowie
- Verfahren über die Verwendung von Adressdaten nach § 47 DSG 2000

Das E-GovG übertrug der Datenschutzbehörde auch noch die Funktion als Stammzahlenregisterbehörde.

Seit 25. Mai 2018 nimmt die Datenschutzbehörde zusätzliche Aufgaben wahr, einige Aufgaben sind weggefallen.

Weggefallen sind insbesondere

- die Führung des Datenverarbeitungsregisters und die damit zusammenhängenden Verfahren nach §§ 17 ff DSG 2000
- ein Großteil der Verfahren betreffend internationalen Datenverkehr (§ 13 DSG 2000)
- die Führung von Kontroll- und Ombudsmannverfahren (§ 30 DSG 2000)

Hinzugekommen sind folgenden Aufgaben:

- die Erlassung von Standardvertragsklauseln zur Heranziehung von Auftragsverarbeitern (Art. 28 DSGVO) unter Einbindung des Europäischen Datenschutzausschusses
- die Entgegennahme und Prüfung von Meldungen über die Verletzung des Schutzes personenbezogener Daten nach Art. 33 DSGVO sowie die Anordnung von Abhilfemaßnahmen
- die Erlassung von Verordnungen betreffend die (Nicht-)Durchführung einer Datenschutz-Folgenabschätzung unter Einbindung des Europäischen Datenschutzausschusses
- die Führung von Konsultationsverfahren nach Art. 36 DSGVO
- die Entgegennahme von Meldungen über die Bestellung von Datenschutzbeauftragten

(Art. 37 Abs. 7 DSGVO)
- die Prüfung und Genehmigung von eingereichten Verhaltensregeln (Art. 40 DSGVO) sowie die Erlassung der korrespondierenden Verordnung über die Akkreditierung von Überwachungsstellen (Art. 41 DSGVO) unter Einbindung des Europäischen Datenschutzausschusses
- Genehmigung von Zertifizierungskriterien (Art. 42 DSGVO) sowie die Erlassung der korrespondierenden Verordnung über die Akkreditierung von Zertifizierungsstellen (Art. 43 DSGVO) unter Einbindung des Europäischen Datenschutzausschusses
- Die Genehmigung von verbindlichen internen Vorschriften (BCR) sowie von Vertragsklauseln zur Übermittlung von Daten an Empfänger in Drittstaaten oder internationalen Organisationen (Art. 46 f DSGVO) unter Einbindung des Europäischen Datenschutzausschusses
- die Führung von Verwaltungsstrafverfahren (Art. 83 DSGVO iVm § 62 DSG)
- die strukturierte Zusammenarbeit mit anderen Aufsichtsbehörden bei grenzüberschreitenden Fällen (Art. 60 f DSGVO)
- die Mitarbeit im Europäischen Datenschutzausschuss (Art. 63 ff DSGVO)

Unverändert hat die Datenschutzbehörde auch nach der neuen Rechtslage
- Beschwerdeverfahren (Art. 77 DSGVO iVm § 24 DSG)
- Amtswegige Prüfverfahren (Art. 57 Abs. 1 lit. h DSGVO)
- Verfahren betreffend die Datenverarbeitung für Zwecke der wissenschaftlichen Forschung und Statistik (§ 7 DSG) sowie die Datenverarbeitung von Adressdaten zur Benachrichtigung und Befragung von betroffenen Personen (§ 8 DSG)

zu führen.

Bis zum Ablauf des 27. Dezember 2018 waren auch noch die Aufgaben als Stammzahlenregisterbehörde wahrzunehmen.

Neben den Aufgaben haben auch die Befugnisse eine Ausweitung erfahren.

Art. 58 DSGVO sieht weitgehende Befugnisse der Aufsichtsbehörden vor. Zu erwähnen sind hier insbesondere
- die Befugnis im Falle einer festgestellten Verletzung der DSGVO Abhilfemaßnahmen anzuordnen, um die Rechtsverletzung abzustellen sowie
- die Befugnis, substantielle Geldbußen bei Verstößen gegen die DSGVO zu verhängen, und zwar zusätzlich zu oder anstelle einer sonstigen Abhilfemaßnahme.

Alle Bescheide der Datenschutzbehörde, deren Anzahl sich aufgrund der zusätzlichen Aufgabengebiete vervielfacht hat, können mit Beschwerde an das Bundesverwaltungsgericht bekämpft werden. Dieses entscheidet auch nach neuer Rechtslage im Dreiersenat (ein Berufsrichter, zwei Laienrichter). Entscheidungen des Bundesverwaltungsgerichtes können – auch von der Datenschutzbehörde – mit Revision an den Verwaltungsgerichtshof bzw. Beschwerde an den Verfassungsgerichtshof bekämpft werden.

Die Datenschutzbehörde stellt auf der Website der DSB allgemeine Informationen zu den Verfahren vor der Datenschutzbehörde sowie Musterformulare für Eingaben zur Verfügung.

Die Entscheidungen der Datenschutzbehörde werden nur dann im RIS veröffentlicht, wenn sie von der bisherigen Rechtsprechung abweichen, es keine Rechtsprechung 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 am Jahresende 2018 34 Personen in Teil- oder Vollzeit ihren Dienst bei der Datenschutzbehörde, davon 21 Juristinnen und Juristen (davon zwei Praktikanten), 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.

Die Vorbereitungen auf die Datenschutz-Grundverordnung (siehe auch Punkt 5 des Berichts), die Bearbeitung der ersten nationalen und internationalen Beschwerden nach der Datenschutzgrundverordnung, die Verfahren betreffend die Data Breach Notifications sowie die Führung der Verwaltungsstrafverfahren zeigen deutlich, dass die Datenschutzbehörde auch 2019 zusätzlichen Personalbedarf hat.

Der Behörde wuchsen neue Aufgaben zu, deren Erfüllung nicht durch den Wegfall des Datenverarbeitungsregisters (und der Arbeit in diesem Bereich), sowie des Wegfalls der Stammzahlenregisterbehörde (hier wurde eine A1 Planstelle dem BMDW übertragen) seit 28. Dezember 2018 kompensiert werden kann.

# 3 Tätigkeit der Datenschutzbehörde

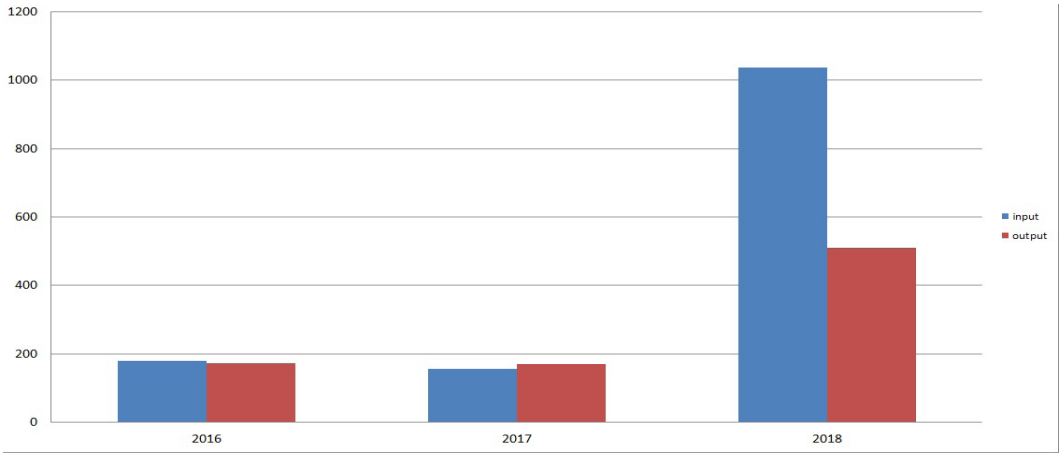
## 3.1 Statistische Darstellung

**Tabelle 1 Anzahl der Eingangsstücke und Erledigungen**

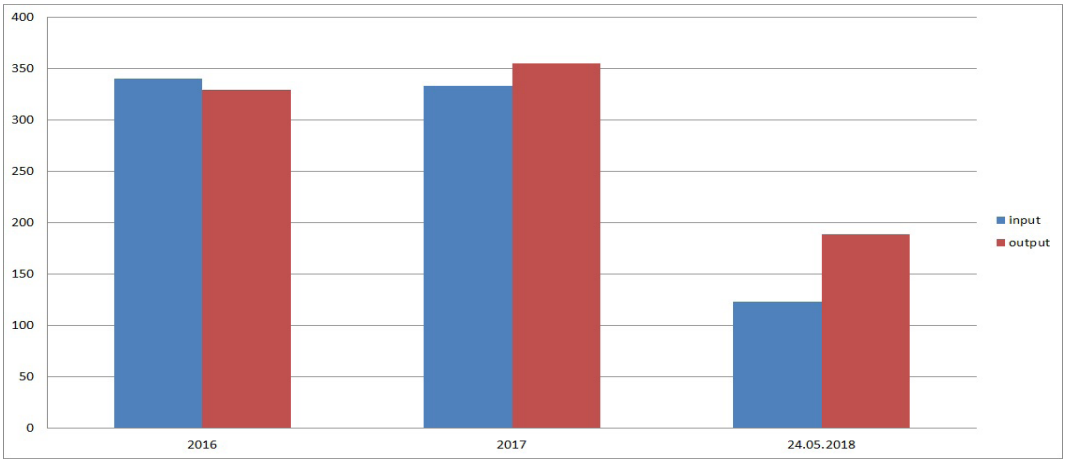
| | Eingangsstücke | | | Erledigungen | | |
|---|---|---|---|---|---|---|
| **Art der Tätigkeit** | **2016** | **2017** | **2018** | **2016** | **2017** | **2018** |
| Individualbeschwerden | 180 | 156 | 1036 | 173 | 170 | 509 |
| Erledigungsart der Individualbeschwerden | | | | 122 Bescheide<br>51 Einstellungen | 115 Bescheide<br>55 Einstellungen | 340 Bescheide<br>169 Einstellungen |
| Beschwerden Grenzüberschreitend seit 25.05.2018 (im Ausland einlangend) | | | 430 | | | 200 |
| Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (Verfahren über Antrag) bis 24.05.2018 | 340 | 333 | 123 | 329 | 355 | 189 |
| Amtswegige Prüfverfahren | 90 | 93 | 129 | 80 | 106 | 95 |
| Genehmigungen nach §§ 46 und 47 DSG 2000 (wissenschaftliche Forschung u Statistik) Antrag gem. §§ 7,8 | 23 | 19 | 17 | 18 | 19 | 23 |
| Genehmigungen im Internationalen Datenverkehr | 312 | 185 | 27 | 254 | 201 | 119 |
| Auskunft Schengen | 20 | 15 | 19 | 20 | 15 | 16 |
| Verwaltungsstrafverfahren seit 25.05.2018 | | | 134 | | | 83 Einstellungen<br>4 Ermahnungen<br>5 Straferkenntnisse |
| Standardvertragsklauseln seit 25.05.2018 | | | 1 | | | 0 |

| Art der Tätigkeit | Eingangsstücke | | | Erledigungen | | |
|---|---|---|---|---|---|---|
| | 2016 | 2017 | 2018 | 2016 | 2017 | 2018 |
| Verfahren vor dem Bundesverwaltungsgericht | 34 | 33 | 50 | | | |
| Sicherheitsverletzungen § 95a | | | 69 | | | 77 |
| Sicherheitsverletzungen Art 33 seit 25.05.2018 | | | 501 | | | 344 |
| Sicherheitsverletzungen grenzüberschreitend seit 25.05.2018 (in Österreich einlangend) | | | 7 | | | 4 |
| Sicherheitsverletzungen grenzüberschreitend seit 25.05.2018 (im Ausland einlangend) | | | 43 | | | 8 |
| Beschwerden grenzüberschreitend seit 25.05.2018 (in Österreich einlangend) | | | 153 | | | 53 |
| Rechtsauskünfte | 2004 | 2239 | 4052 | 1980 | 2192 | 3974 |
| Anträge auf Genehmigung von Verhaltensregeln seit 25.05.2018 | | | 8 | | | 1 |
| Konsultationsverfahren seit 25.05.2018 | | | 2 | | | 2 |
| Verkehr mit Behörden | | | 226 | | | 226 |
| Bescheide im Registrierungsverfahren bis 24.05.2018 | 4 | 8 | 1 | 3 | 1 | 1 |
| Verfahren gem. § 22a DSG 2000 bis 24.05.2018 | 2 | 8 | 1 | 2 | 8 | 1 |
| Rechtsunwirksam eingebracht bis 24.05.2018 | 57 | 96 | 38 | 104 | 96 | 38 |
| Meldungen von Rechtsnachfolgen bis 24.05.2018 | 802 | 1014 | 23 | 57 | 91 | 23 |

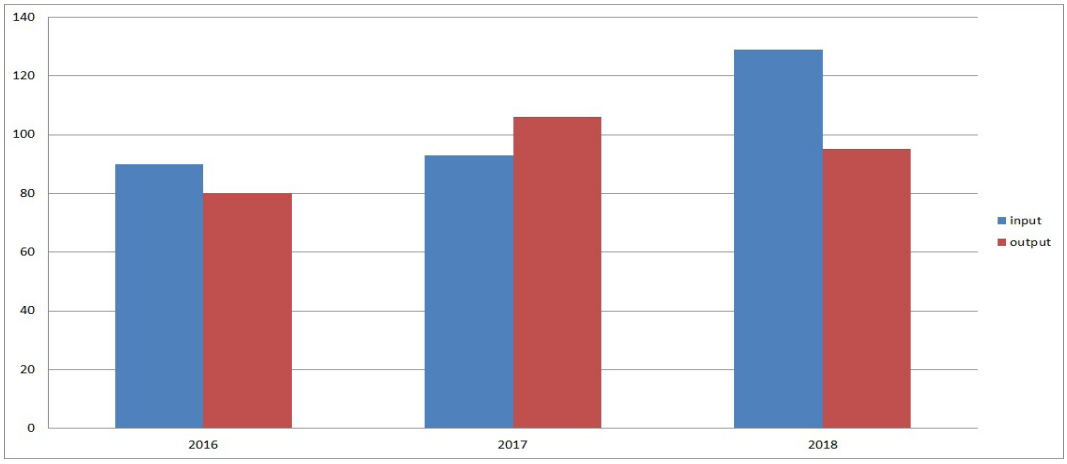
## Individualbeschwerden



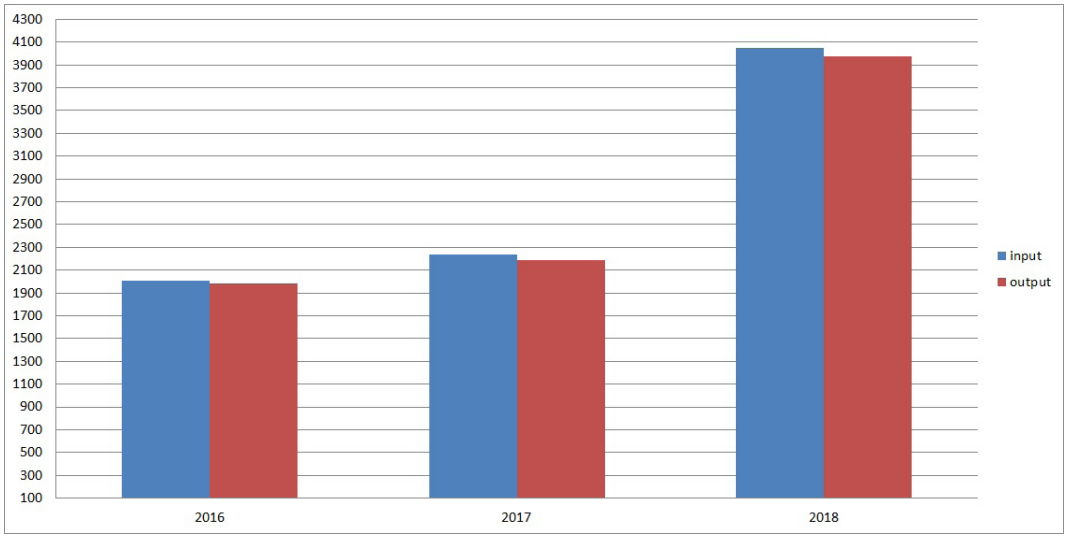

## Kontroll- und Ombudsmannverfahren (§ 30 DSG 2000)



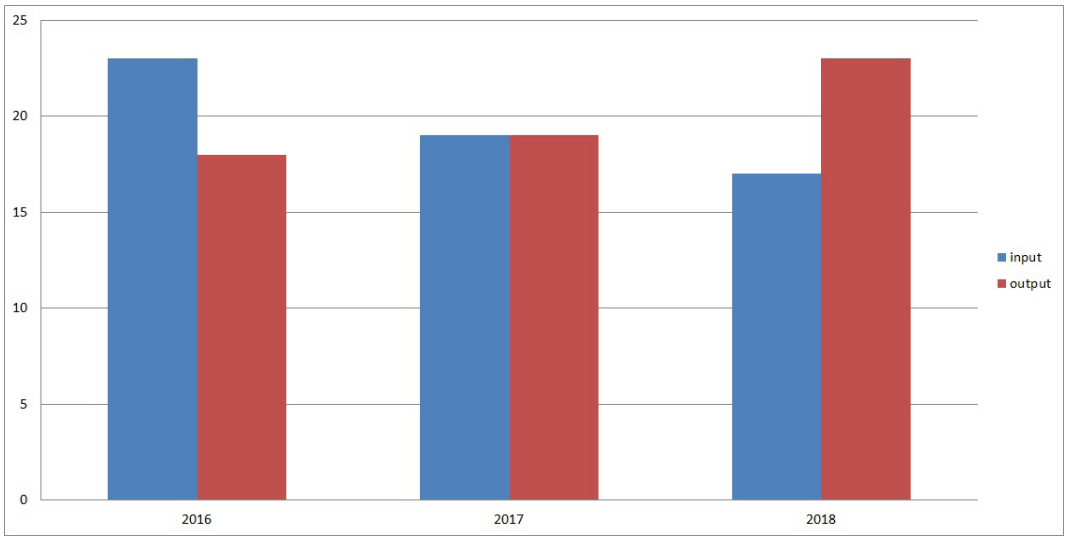
## Amtswegiges Prüfverfahren



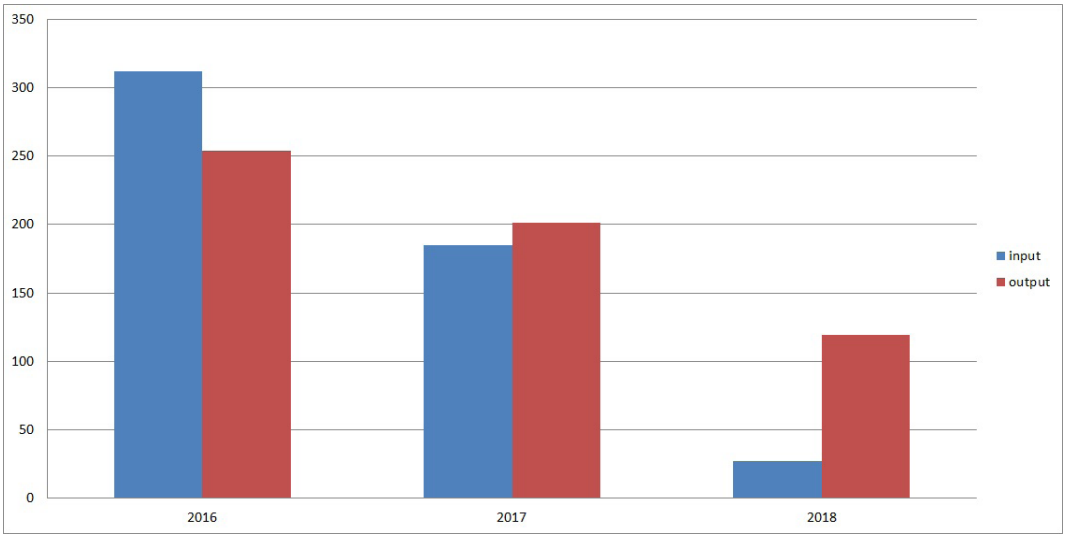

## Rechtsauskünfte



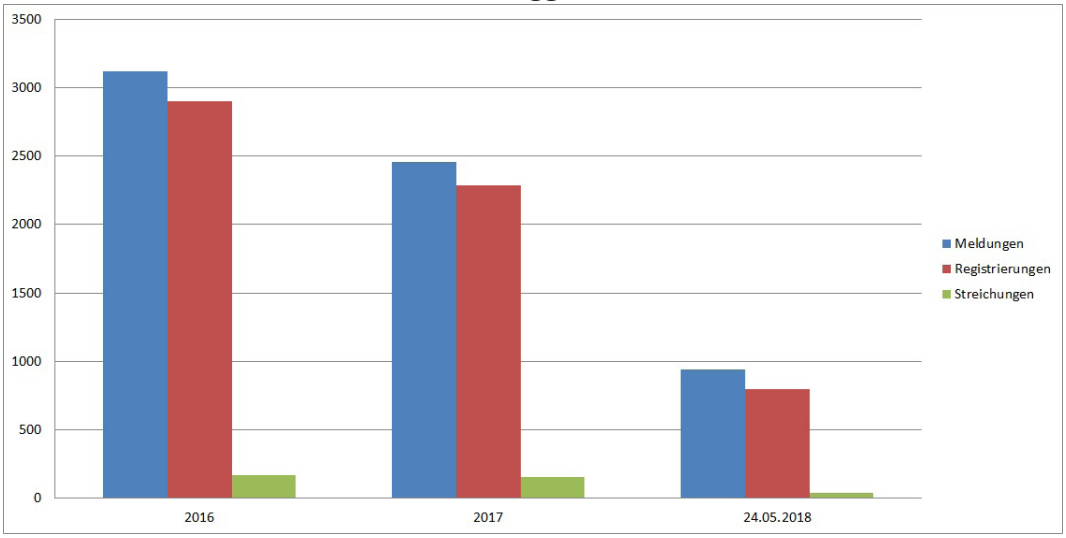

## Genehmigungen nach §§ 46,47 DSG 2000 und Antrag gem. §§7,8



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




**Auftraggeber**




**Datenanwendungen**

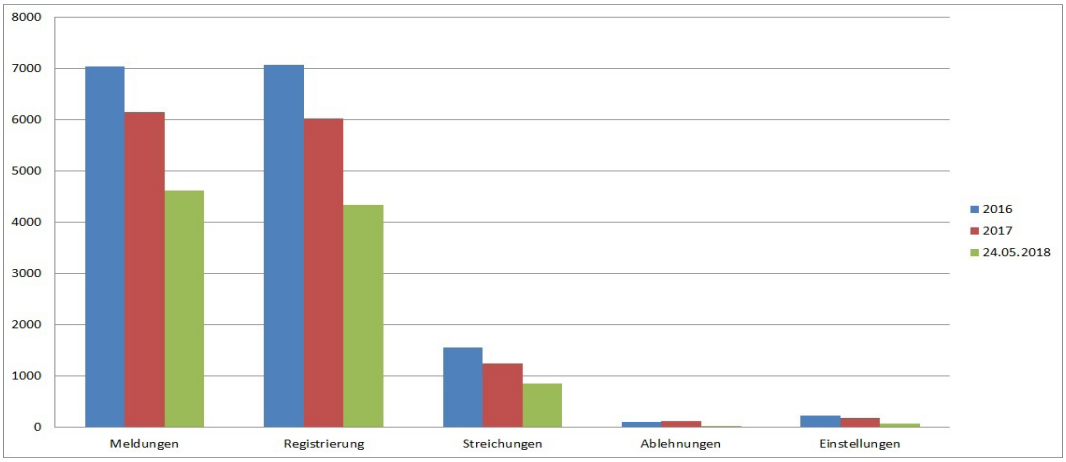


**Tabelle 2 Anzahl der Tätigkeiten des Datenverarbeitungsregisters**

| Tätigkeiten | 2016 | 2017 | 01.01. - 24.05.2018 |
|---|---|---|---|
| **Tätigkeiten für Auftraggeber in Summe** | **6186** | **4898** | **1777** |
| Meldungen | 3119 | 2455 | 939 |
| Registrierungen | 2901 | 2290 | 798 |
| *davon automatisch registriert* | *2135 (ca. 73 %)* | *1540 (ca. 67 %)* | *594 (ca. 75 %)* |
| *davon durch das DVR registriert* | *766 (ca. 27 %)* | *750 (ca. 33 %)* | *204 (ca. 25 %)* |
| Streichungen | 166 | 153 | 40 |
| **Tätigkeiten in Datenanwendungen in Summe** | **16007** | **13703** | **9914** |
| Meldungen | 7045 | 6154 | 4617 |
| *davon automatisch registriert* | *4300 (ca. 61 %)* | *3432 (ca. 56 %)* | *1363 (ca. 30 %)* |
| *davon vom DVR überprüft* | *2745 (ca. 39 %)* | *2722 (ca. 44 %)* | *3254 (ca. 70 %)* |
| Registrierungen | 7072 | 6016 | 4343 |
| Streichungen | 1558 | 1239 | 856 |
| Ablehnungen | 105 | 115 | 25 |
| Einstellungen | 227 | 179 | 73 |
| **Verbesserungsaufträge in Summe** | **1009** | **1000** | **210** |
| Bescheide im Registrierungsverfahren | 3 | 1 | 1 |
| Verfahren gemäß § 22a DSG 2000 | 2 | 8 | 1 |
| Rechtsunwirksam eingebrachte Meldungen | 104 | 96 | 38 |
| Meldungen von Rechtsnachfolgen | 57 | 91 | 23 |

## 3.2 Verfahren und Auskünfte

### 3.2.1.1 Individualbeschwerden

**Allgemeines und Grundsätzliches**

Das Beschwerdeverfahren nach § 31 DSG 2000 (bis 25. Mai 2018) und § 24 DSG iVm Art. 77 DSGVO (seit 25. Mai 2018) ist das wichtigste Rechtsschutzverfahren zur Durchsetzung von Betroffenenrechten.

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

Die nationale Begleitgesetzgebung zur DSGVO hat in § 24 DSG, an bisherige bewährte Regelungen in § 31 DSG 2000 anknüpfend, das Beschwerderecht verfahrensrechtlich als Recht auf ein förmliches Rechtsschutzverfahren ausgestaltet, in dem die Datenschutzbehörde streitentscheidend und daher grundsätzlich unparteiisch tätig wird. Der betroffenen Person wird in der Rolle des Beschwerdeführers dabei mehr abverlangt als das Verfassen eines mehr oder weniger umfangreichen Beschwerdeschreibens. Bedingt ist dies durch die verfahrensrechtliche Vorgabe, dass ein abgrenzbarer Sachverhalt mit möglichst genau feststehenden Beteiligten (eine „Verwaltungssache“ im Sinne des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG) dargelegt werden muss, den die Datenschutzbehörde als Rechtsschutzbehörde untersuchen und rechtlich zu beurteilen hat. Die Datenschutzbehörde hat zur Erleichterung dieser Anforderungen u.a. verschiedene leicht verständliche Formulare auf ihrer Website zur Verfügung gestellt, deren Verwendung sicherstellen soll, dass eine Beschwerde nicht an verfahrensrechtlichen Formalitäten scheitert. Die Form- und Inhaltserfordernisse des § 24 Abs. 2 und 3 DSG werden nämlich streng gehandhabt. Wer entsprechende Mängel (etwa das Fehlen des Nachweises eines gestellten Antrags auf Auskunft oder Löschung) nicht binnen einer gesetzten Frist beheben kann, muss mit der Zurückweisung seiner Beschwerde rechnen (siehe auch Entscheidungen h) und l) unten).

Gegen Ende des Jahres 2018 wurde aufgrund erster Erfahrungen begonnen, die Formulare zweisprachig (deutsch mit englischer Übersetzung) zu gestalten, um ihre Verwendung in den Verfahren gemäß Kapitel VII DSGVO zu erleichtern, da dort Englisch als Arbeitssprache verwendet wird. Gleichzeitig wurde dabei auf barrierefreie Gestaltung und die Möglichkeit zur Anbringung einer elektronischen Signatur Bedacht genommen. Die Beschwerde ist jedoch auf Deutsch einzubringen (Art. 8 B-VG).

Während sich bis 25. Mai 2018 die Zuständigkeit der Datenschutzbehörde zur Durchsetzung subjektiver Rechte im privaten Bereich nur auf das Recht auf Auskunft erstreckte, kann die Zuständigkeit nunmehr so beschrieben werden:

Die Datenschutzbehörde ist im Inland für Beschwerden gegen alle Rechtsträger öffentlichen und privaten Rechts zuständig, die personenbezogene Daten verarbeiten, ausgenommen sind die folgenden Gebiete:

- die Gesetzgebung von Bund und Ländern (samt zugeordneten Prüforganen wie Rechnungshof und Volksanwaltschaft),
- die Gerichtsbarkeit, soweit sie judizielle Aufgaben (Streitentscheidung in Mehrparteienverfahren unter dem Schutz der richterlichen Unabhängigkeit) wahrnimmt,
- Datenverarbeitungen, die durch natürliche Personen ausschließlich zur Ausübung

persönlicher oder familiärer Tätigkeiten vorgenommen werden, und
- Datenverarbeitungen für Zwecke der Medienberichterstattung und für Zwecke, die vom Grundrecht auf Informations- und Meinungsfreiheit geschützt sind (siehe unten Entscheidung j).

Hinsichtlich der Zuständigkeit der Datenschutzbehörde für Beschwerden im Bereich der Justizbehörden, insbesondere der Staatsanwaltschaften, bestehen einige Fragen betreffend die Auslegung von Art. 55 Abs. 3 DSGVO und § 31 Abs. 1 2. Satz DSG. Diese werden voraussichtlich in den nächsten Jahren durch die Verwaltungsgerichte geklärt werden.

Beim Beschwerdeverfahren handelt es sich, wie bereits erwähnt, um ein Verwaltungsverfahren nach dem AVG. Es wird abgegrenzt von einem eventuell anschließenden Verwaltungsstrafverfahren geführt. Auf Grund der Ergebnisse des Beschwerdeverfahrens, einbeziehend das Verhalten des Beschwerdegegners, wird regelmäßig entschieden, ob auch die Einleitung eines Verwaltungsstrafverfahrens erforderlich ist. Im Beschwerdeverfahren besteht gemäß Art. 31 DSGVO für Verantwortliche und Auftragsverarbeiter eine – durch Geldbußen sanktionierbare – Pflicht, mit der Datenschutzbehörde zusammenzuarbeiten.

Gemäß Art. 80 Abs. 1 DSGVO können sich betroffene Personen vor der Datenschutzbehörde durch Organisationen ohne Gewinnerzielungsabsicht vertreten lassen, die Datenschutz als satzungsmäßigen Zweck verfolgen. Dies war auch vor dem 25.5.2018 möglich. Das in Art. 80 Abs. 2 DSGVO als Option vorgesehene Recht solcher Organisationen, auch ohne Auftrag und Vollmacht Betroffener Beschwerden einzubringen (Verbandsbeschwerde), ist in Österreich nicht vorgesehen.

Der Datenschutzbehörde kommt von Gesetzes wegen im Beschwerdeverfahren nach alter wie neuer Rechtslage die Rolle einer unabhängigen Streitentscheidungsinstanz zu (§ 31 Abs. 1, 2 und 7, § 37 Abs. 1 DSG 2000, seit 25. Mai 2018 nunmehr Art. 57 Abs. 1 lit. f und Art. 77 DSGVO, § 24 Abs. 1 und 5, § 32 Abs. 1 Z 4 DSG). Die Entscheidungen im Verfahren werden durch die Leiterin der DSB oder in ihrem Namen durch ihren Stellvertreter oder einen aufgrund einer Ermächtigung handelnden Vertreter („Genehmiger“) getroffen. Die ermächtigten Vertreter sind an allfällige Weisungen der Leiterin gebunden.

Im Verfahren wegen Verletzung der Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Unterlassung automatisierter Einzelfallentscheidungen nach der DSGVO muss dem Beschwerdeverfahren vor der Datenschutzbehörde zwingend ein „Vorverfahren“ zwischen der betroffenen Person und dem Verantwortlichen vorangegangen sein, in dem Erstere das jeweilige Recht geltend gemacht hat. Die Ausübung des Rechts muss der Datenschutzbehörde bei Beschwerdeerhebung nachgewiesen werden (§ 24 Abs. 3 DSG).

Das Verfahren zur Durchsetzung der Rechte der betroffenen Person bei Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs (3. Hauptstück des DSG, keine direkte Anwendung der DSGVO) ist in etwas stärkerem Maß durch die Möglichkeit der Datenschutzbehörde geprägt, als Aufsichtsbehörde nicht nur streitentscheidend tätig zu werden, sondern auch im Interesse der betroffenen Person aktiv in das Verfahren einzugreifen („kommissarischer Rechtsschutz“, vgl. insbesondere § 42 Abs. 8 und 9 DSG). Eine Erprobung dieser neuen Rechtsschutzinstrumente erfolgte 2018 nicht.

### Praxis der Beschwerdeverfahren im Jahr 2018

Das Berichtsjahr ist durch ein mit Wirksamwerden der DSGVO ab dem 25. Mai 2018 einsetzendes massives Ansteigen der Zahl der eingebrachten Beschwerden gekennzeichnet.

Details enthält das Kapitel Statistik. Selbst bei Zusammenrechnung der Zahlen nach den §§ 30 und 31 DSG 2000 für die Vorjahre ist von einer mehr als Verdreifachung des Anfalls auszugehen, wobei es sich nunmehr ausschließlich um Verfahren handelt, die gemäß § 73 Abs. 1 AVG längstens innerhalb von sechs Monaten durch einen Bescheid abgeschlossen werden müssen.

Im Berichtsjahr konzentrierten sich die Beschwerdeverfahren auf die Rechte auf Auskunft, Geheimhaltung, Berichtigung/Löschung und Widerspruch. Das in § 1 DSG normierte nationale Grundrecht auf Geheimhaltung bildet in der Praxis dabei den Rahmen, innerhalb dessen die „Grundsätze" gemäß Kapitel II der DSGVO wie ausdrückliche Betroffenenrechte gemäß Kapitel III der DSGVO geltend gemacht werden können. Die in Kapitel III der DSGVO geregelten Rechte auf Einschränkung (Art. 18 DSGVO), Datenübertragbarkeit (Art. 20 DSGVO) und Unterlassung automatisierter Einzelfallentscheidungen (Art. 22 DSGVO) haben im Berichtszeitraum noch keine Bedeutung erlangt.

Die durch die DSG-Novelle 2010 eingeführte Möglichkeit, Beschwerdeverfahren als „gegenstandslos" durch Einstellung zu beenden (bis 25. Mai 2018 § 31 Abs. 8 DSG 2000), wurde auch in die verfahrensrechtlichen Bestimmungen im DSG übernommen (nunmehr § 24 Abs. 6 DSG). Sie ermöglicht es insbesondere, Beschwerdeverfahren wegen Auskunfts- oder Löschungsanträgen, auf die der Verantwortliche in gesetzwidriger Weise zunächst nicht reagiert hat, nach Erreichung des primären Verfahrensziels (Beantwortung des Auskunfts- oder Löschungsantrags) ohne großen Aufwand zu beenden. Diese Form der Verfahrensbeendigung wegen Klaglosstellung wurde nach alter Rechtslage mehrfach durch das Bundesverwaltungsgericht als rechtmäßig bestätigt. Eine solche Einstellung des Beschwerdeverfahrens schützt den Verantwortlichen jedoch, insbesondere in Fällen wiederholter Verstöße gegen die in Art. 12 Abs. 4 DSGVO festgelegten Fristen zur Umsetzung von Betroffenenrechten, nicht vor möglichen verwaltungsstrafrechtlichen Folgen.

### Ausgewählte Beschwerdeentscheidungen aus 2018

Die DSB hat in ihrer öffentlich zugänglichen Entscheidungsdokumentation (im Rahmen des Rechtsinformationssystems des Bundes – RIS; Stand: 5. Februar 2019) aus dem Jahr 2018 siebzehn Bescheide aus Beschwerdeverfahren dokumentiert, darunter auch „Übergangsverfahren", die als Kontroll- und Ombudsmannverfahren nach § 30 DSG 2000 begonnen und gemäß § 69 Abs. 4 DSG als Beschwerdeverfahren fortgeführt und beendet worden sind. Diese Zahl wird sich aus verschiedenen Gründen (z.B. wegen abzuwartender Rechtsmittelentscheidungen des BVwG, VfGH oder VwGH) auch nach Erscheinen des Datenschutzberichts 2018 noch ändern.

Regelmäßig werden nur rechtskräftige Entscheidungen dokumentiert, Ausnahmefälle sind in den RIS-Dokumenten durch entsprechende Vermerke gekennzeichnet. In solchen Fällen wird die Entscheidung nach einer Aufhebung durch das Bundesverwaltungsgericht aus dem RIS entfernt oder der sonstige Ausgang des Verfahrens dokumentiert. Nicht alle im RIS dokumentierten Entscheidungen scheinen in der nachfolgenden Übersicht auf.

Über andere, insbesondere nicht rechtskräftige Entscheidungen, wurde im Newsletter der Datenschutzbehörde berichtet.

**Die wichtigsten Beschwerdeentscheidungen in chronologischer Reihenfolge:**

**a. Bescheid vom 22.1.2018, GZ: DSB-D122.767/0001-DSB/2018 (datenschutzrechtliche Rolle einer Steuerberatungsgesellschaft, rechtskräftig, RIS)**

In dieser Sache verlangte ein Betroffener Auskunft zu seinen Daten von einer Steuerberatungsgesellschaft m.b.H. & Co KG, die für seinen Dienstgeber (eine Bundesdienststelle) die Lohn-

verrechnung durchführte. Er erhielt zunächst keine Antwort (u.a. da das Auskunftsverlangen im E-Mail-System der Empfängerin vom SPAM-Filter erfasst wurde). Nach Einbringung der Beschwerde brachte die nunmehrige Beschwerdegegnerin gegen das Beschwerdevorbringen im Kern vor, als Dienstleisterin (in der Terminologie der DSGVO nunmehr: Auftragsverarbeiterin) gar nicht zur Auskunft verpflichtet zu sein. Die Datenschutzbehörde hielt dazu fest, dass Wirtschaftstreuhänder, zu denen auch die Steuerberater zählen, gesetzlich über eine berufliche Rechtsstellung verfügen, die die eigenverantwortliche Auftragserfüllung gegenüber dem Mandanten betont. Es war daher, wie bei Rechtsanwälten, davon auszugehen, dass diese bei der Besorgung von Geschäften für ihre Mandanten gemäß § 4 Z 4 letzter Halbsatz DSG 2000 „eigenverantwortlich" vorgehen dürfen und damit hinsichtlich der zwecks Auftragserfüllung verarbeiteten personenbezogenen Daten Auftraggeber (in der Terminologie der DSGVO nunmehr: für die Verarbeitung Verantwortliche) sind. Der Beschwerde wurde daher Folge gegeben.

**b. Bescheid vom 16.2.2018, GZ: DSB-D122.757/0002-DSB/2018 (Löschung von Daten über ein anhängiges Ermittlungsverfahren bei der Führerscheinbehörde, rechtskräftig, Newsletter 2/2018, Seite 3)**

Im diesem Bescheid hatte sich die Datenschutzbehörde mit der Frage zu beschäftigen, ob die Führerscheinbehörde Daten über ein anhängiges Ermittlungsverfahren betreffend den Beschwerdeführer zu löschen hatte. Konkret übermittelte eine Landespolizeidirektion Daten über ein anhängiges Ermittlungsverfahren gegen den Beschwerdeführer an die Beschwerdegegnerin in ihrer Funktion als Sicherheits- und Führerscheinbehörde. Die Beschwerdegegnerin legte diese Information über ein anhängiges Ermittlungsverfahren anschließend ihrer Beurteilung zur Verkehrsunzuverlässigkeit des Beschwerdeführers zu Grunde. Der Beschwerdeführer begehrte die Löschung dieser Daten betreffend das gegen ihn anhängige Ermittlungsverfahren, da für diese Übermittlung seiner Daten keine Rechtsgrundlage vorliegen würde. Die Beschwerdegegnerin lehnte das Löschbegehren jedoch mit der Begründung ab, dass sie als Führerscheinbehörde eine Verkehrsunzuverlässigkeit bei erwiesenen, bestimmten Tatsachen annehmen dürfe. Was jedoch unter „erwiesen" zu verstehen sei, stünde der Beschwerdegegnerin zur Beurteilung frei. Die Beschwerdegegnerin brachte darüber hinaus vor, dass sie die Begehung einer strafbaren Handlung als Vorfrage für die Entziehung der Lenkberechtigung gemäß § 38 AVG nach der eigenen Anschauung beurteilen müsse.

Im Ergebnis war dem Beschwerdeführer Recht zu geben: Bei Daten betreffend ein anhängiges Ermittlungsverfahren handelt es sich um „Strafdaten" im Sinne des § 8 Abs. 4 DSG 2000, für die ein besonderer datenschutzrechtlicher Schutz vorgesehen ist. Demnach muss für „Strafdaten" eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung vorliegen. Nach dem klaren Wortlaut des Führerscheingesetzes wird eine Verkehrsunzuverlässigkeit nur bei (gewissen) erwiesenen strafbaren Handlungen angenommen. Der bloße Verdacht reicht hierfür nicht aus. Die Datenschutzbehörde folgt somit der Judikatur des Verwaltungsgerichtshofs (siehe dazu die Erkenntnisse des Verwaltungsgerichtshofes vom 23. Mai 2005, Zl. 2000/11/0065, und vom 16. Oktober 2012, Zl. 2012/11/0171, beide in Bezug auf § 7 Abs. 3 Z 1 Führerscheingesetz).

Da im gegenständlichen Fall zum Zeitpunkt des Empfangs der gegenständlichen strafrechtsrelevanten Daten lediglich der Verdacht bestand, der Beschwerdeführer könnte die einschlägigen strafbaren Handlungen begangen haben, lehnte die Beschwerdegegnerin das Löschbegehren des Beschwerdeführers zu Unrecht ab. Darüber hinaus wurde der Beschwerdeführer im Laufe des Verfahrens vor der Datenschutzbehörde auch von den gegen ihn erhobenen Vorwürfen rechtskräftig freigesprochen. Es war folglich eine Verletzung im Recht auf Löschung festzustellen. Dieser Bescheid ist rechtskräftig.

Die Frage der Zulässigkeit der Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten richtet sich nunmehr nach Art. 10 DSGVO und den entsprechenden Materiengesetzen.

**c. Bescheid vom 17.4.2018, GZ: DSB-D122.848/0004-DSB/2018 (Ladung samt Zustellverfügung und deren Vollzug als Akt der Gerichtsbarkeit, Unzuständigkeit der DSB, rechtskräftig, RIS)**

Die Beschwerdeführerin wurde von einem Bezirksgericht in einer familienrechtlichen Sache vorgeladen. Die Ladung wurde, entsprechend der vom zuständigen Richter im Aktenverwaltungssystem VJ genehmigten Zustellverfügung, als ein Schriftstück in einem Fensterkuvert zugestellt, wobei im Fenster des Kuverts neben ihrem Namen und der Adresse auch ihr Geburtsdatum, ihr Beruf und der Hinweis „Nicht an den Ehepartner oder Gatten abzugeben" angeführt waren. Die Beschwerdeführerin sah dadurch ihr Geheimhaltungsrecht als verletzt. Da das richterliche Organ – trotz Vorgaben durch das Aktenverwaltungssystem VJ – Einfluss auf die in der Zustellverfügung anzuführenden Daten nehmen konnte, konnte der Zustellmodus zumindest als vom Richter bestätigt angesehen werden. Damit war der Zustellvorgang eine gemäß § 31 Abs. 2 DSG 2000 der Zuständigkeit der Datenschutzbehörde entzogene Datenverarbeitung im Dienste der Gerichtsbarkeit. Die Beschwerde wurde daher zurückgewiesen und die Beschwerdeführerin auf das Rechtsschutzverfahren nach den §§ 83 und 85 GOG verwiesen.

**d. Bescheid vom 13.5.2018, GZ: DSB-D122.815/0003-DSB/2018 (Unzulässigkeit der mündlichen Übermittlung der Daten eines Schwarzfahrers durch Polizeibeamte an ein Verkehrsunternehmen, rechtskräftig, RIS)**

Der Beschwerdeführer wurde bei einer Fahrausweiskontrolle in der Wiener U-Bahn von den Kontrollorganen des Verkehrsunternehmens ohne Fahrschein oder Zeitkarte angetroffen und weigerte sich, seine Identitätsdaten anzugeben. Die Kontrollorgane verständigten die Bundespolizei, deren Beamte eine Identitätsfeststellung wegen des Verdachts einer Verwaltungsübertretung nach Art. III Abs. 1 Z 2 EGVG („Schwarzfahren") durchführten. Gegen den ausdrücklichen Widerspruch des Beschwerdeführers wurden sein Name, sein Geburtsdatum und seine Adresse darauf mündlich an die noch anwesenden Kontrollorgane des Verkehrsunternehmens übermittelt. Die anschließende Beschwerde wegen Verletzung des Geheimhaltungsrechts richtete sich gegen die Landespolizeidirektion Wien und erwies sich als berechtigt. Es handelte sich bei den Daten um auf Grund hoheitlicher Befugnisse von der Sicherheitsbehörde erhobene „Strafdaten" gemäß § 8 Abs. 4 DSG 2000, die in Ermangelung einer ausdrücklichen gesetzlichen Ermächtigung (eine solche findet sich weder im EGVG, noch im VStG oder SPG) hier nicht an Dritte übermittelt werden hätten dürfen. Das berechtigte Interesse des Verkehrsunternehmens an den Daten (wegen Durchsetzung möglicher zivilrechtlicher Ansprüche) reichte hier nicht. Auch das von der Beschwerdegegnerin als Grundlage angeführte Auskunftspflichtgesetz war hier keine taugliche Grundlage für den Eingriff in das Geheimhaltungsrecht.

**e. Bescheid vom 28.5.2018, GZ: DSB-D216.580/0002-DSB/2018 (Löschung, kein Recht des Verantwortlichen auf vorsorgliche Speicherung von Kontaktdaten, rechtskräftig, RIS, Newsletter 3/2018, Seite 2 f)**

In diesem Bescheid in einem Übergangsfall hatte sich die Datenschutzbehörde mit der Notwendigkeit der Speicherung von personenbezogenen Daten zu befassen. Der Beschwerdeführer verlangte von dem Beschwerdegegner die Löschung sämtlicher seine Person betreffenden Daten, nachdem dieser zwar einem vorangegangen ersten Antrag auf Löschung des Beschwerdeführers entsprochen hatte, im Zuge dessen jedoch erneut Vor- und Zuname, Geburtsdatum, sowie aktuelle Adresse des Beschwerdeführers speicherte. Begründet wurde dies von dem Beschwerdegegner mit einem Verweis auf eine Speicherung aus „sicher amtsbekannten Gründen" nach Art. 17 Abs. 3 lit. e DSGVO sowie der Notwendigkeit für Dokumentations- und

Kommunikationszwecke. Die Datenschutzbehörde gab der Beschwerde statt und hielt fest, dass die Berufung auf „sicher amtsbekannte Gründe“ keinen ausreichenden Beweis für die Erforderlichkeit der Verarbeitung nach Art. 17 Abs. 3 DSGVO darstellt. Insbesondere ist aufgrund eines Antrages auf Löschung sämtlicher Daten die Speicherung im Hinblick auf eine eventuell zukünftige Kontaktaufnahme gemäß Art. 17 Abs. 1 lit. a DSGVO nicht notwendig und widerspricht überdies dem Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO.

**f. Bescheid vom 28.5.2018, GZ: DSB-D216.471/0001-DSB/2018 (Geheimhaltung, Telekom-Unternehmen, gesetzlich zulässiger Speicherzeitraum von Stammdaten und Verkehrsdaten, rechtskräftig, RIS, Newsletter 3/2018, Seite 3)**

In diesem Bescheid, ebenfalls in einem Übergangsfall ergangen, hatte sich die Datenschutzbehörde mit der gesetzlich zulässigen Dauer der Speicherung von Stammdaten, Verkehrsdaten und darüberhinausgehenden personenbezogenen Daten durch ein Telekommunikationsunternehmen zu befassen. Die Beschwerdeführerin machte ihr Recht auf Geheimhaltung geltend und führte aus, dass die Beschwerdegegnerin auch nach Beendigung der Vertragsverhältnisse ihre oben genannten Daten unzulässigerweise speichere. Die Beschwerdegegnerin begründete die Speicherung von Stammdaten für einen Zeitraum von zehn Jahren nach Beendigung der Vertragsverhältnisse mit der gesetzlichen Verpflichtung nach § 207 Abs. 2 BAO. Die Speicherung von Verkehrsdaten für einen Zeitraum von sechs Monaten nach Durchführung des Bezahlvorganges stützte sie auf § 99 Abs. 2 TKG 2003. Die Datenschutzbehörde gab der Beschwerde statt und hielt fest, dass § 207 Abs. 2 BAO lediglich eine Verjährungsfrist, jedoch keine konkrete Verpflichtung zur Aufbewahrung von Daten normiert und daher nicht zur längeren Speicherung aufgrund im öffentlichen Interesse liegender Archivzwecke gemäß Art. 5 Abs. 1 lit. e DSGVO berechtigt. Stammdaten sind daher gemäß § 132 Abs. 1 BAO zulässigerweise nur für eine Dauer von sieben Jahren aufzubewahren. Zudem kann die gesetzliche Frist des § 99 Abs. 2 TKG 2003 von drei Monaten nicht mit der Berufung auf interne Prozesse bzw. den Postlauf auf insgesamt sechs Monate ausgedehnt werden. Darüberhinausgehende personenbezogene Daten sind jedenfalls nach Beendigung der Vertragsverhältnisse entsprechend dem Grundsatz der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO zu löschen. Ein entsprechender Löschungsauftrag wurde ebenfalls im Bescheid ausgesprochen.

**g. Bescheid vom 6.6.2018, GZ: DSB-D122.829/0003-DSB/2018 (Auskunft, Recht der betroffenen Person auf Offenlegung des Datenempfängers bei unrechtmäßigen Abfragen, rechtskräftig, RIS)**

Grundsätzlich besteht nach der Rechtsprechung bei internen Verarbeitungsvorgängen (z.B. Abfrage, Eingabe, Abspeichern von Daten) kein Recht der betroffenen Person auf Auskunft darüber, welcher Mitarbeiter eines Verantwortlichen die Verarbeitung vorgenommen hat, selbst wenn entsprechende Protokolldaten vorliegen. In diesem Beschwerdefall (siehe auch den zusammenhängenden Bescheid vom 4.6.2018, GZ: DSB-D122.831/0003-DSB/2018) hat die Datenschutzbehörde jedoch erstmals angeordnet, dass der Verantwortliche für die Datenverarbeitungen einer öffentlichen Krankenanstalt der Beschwerdeführerin, einer Mitarbeiterin dieser Krankenanstalt, offenlegen muss, wer bestimmte, unrechtmäßige Abfragen der Krankengeschichte der Beschwerdeführerin vorgenommen hat. Grund dafür war, dass unbegründete und daher unrechtmäßige Abfragen gemäß Art. 15 Abs. 1 lit. c DSGVO als Übermittlungen zu beauskunften sind.

**h. Bescheid vom 21.6.2018, GZ: DSB-D122.844/0006-DSB/2018 (Auskunft, Bank, Recht der betroffenen Person auf kostenlose Auskunft über verarbeitete Kontoführungsdaten, nicht rechtskräftig)**

Der Beschwerdeführer richtete (vor Wirksamwerden der DSGVO) ein Auskunftsverlangen an die Beschwerdegegnerin, eine Bank-AG, und begehrte Auskunft über eigene Daten, speziell über Überweisungen der Jahre zurück bis 2013, die er nicht mehr über e-banking einsehen

könne. Die Beschwerdegegnerin hat keine datenschutzrechtliche Auskunft erteilt und knüpfte eine Auskunft an die Bezahlung von Kosten in Höhe von EUR 30,-- pro Jahr.

Die Datenschutzbehörde befand die erhobene Beschwerde für begründet und wies die Beschwerdegegnerin an, Auskunft zu erteilen. Es besteht keine speziellere gesetzliche Regel zur Auskunftspflicht einer Bank als Art. 15 DSGVO (die Beschwerdegegnerin hatte sich hierzu auf das Zahlungsdienstegesetz 2018 berufen). Da der Beschwerdeführer überdies zum ersten Mal im laufenden Jahr Auskunft verlangt und den Antrag auf Auskunft zweckmäßig eingeschränkt hatte, gehe auch der Einwand der Schikane ins Leere. Es bestand daher kein Recht der Bank auf Kostenersatz oder Auskunftsverweigerung gemäß Art. 12 Abs. 5 lit. a und b DSGVO.

Gegen diesen Bescheid hat die Bank Beschwerde an das Bundesverwaltungsgericht erhoben.

**i. Bescheid vom 2.8.2018, GZ: DSB-D130.006/0002-DSB/2018 (Verfahrensrecht, Beschwerde gegen ausländischen Suchmaschinenbetreiber bei Fehlen eines Nachweises der Ausübung des Löschungsrechts unzulässig, rechtskräftig, RIS)**

Der Beschwerdeführer wollte sein Löschungsrecht gegen den Betreiber einer großen Internet-Suchmaschine geltend machen (näherer Grund war eine dort angebotene Funktion zur automatischen Ergänzung des Namens des Beschwerdeführers mit weiteren Vorschlägen für Suchbegriffe). Der Beschwerdeführer legte keinen an den Verantwortlichen gerichteten Löschungsantrag vor. Nach einem Mangelbehebungsantrag der Datenschutzbehörde brachte er vor, den entsprechenden Antrag auf der „Support Seite" des Verantwortlichen gestellt zu haben, dies jedoch „nicht schriftlich" sondern über eine „vordefinierte elektronische Maske". Die Datenschutzbehörde wies die Beschwerde dennoch gemäß § 13 Abs. 3 AVG iVm § 24 Abs. 3 DSG zurück. Die Frage, ob das Recht auf Löschung bzw. „Vergessenwerden" gemäß Art. 17 DSGVO auch ein Recht auf Unterdrückung bestimmter automatischer Suchvorschläge umfasse, sei neu und rechtlich noch unbeantwortet, daher wäre es aus Sicht der Datenschutzbehörde von entscheidender Bedeutung gewesen, den genauen Wortlaut des an den Verantwortlichen gerichteten Antrags zu kennen. Dass der Beschwerdeführer das entsprechende Dokument nach eigenen Angaben weder erstellt noch gesichert habe, gehe zu seinen Lasten.

**j. Bescheid vom 13.8.2018, GZ: DSB-D123.077/0003-DSB/2018 (kein Recht auf Löschung von Foren-Beiträgen unterhalb eines Online-Zeitungsartikels, rechtskräftig, RIS, Newsletter 4/2018, Seite 3)**

In diesem Bescheid hatte sich die Datenschutzbehörde mit der Frage zu beschäftigten, ob ein Recht auf Löschung von Beiträgen einer betroffenen Person besteht, die diese im Rahmen eines Diskussionsforums unterhalb eines Online-Zeitungsartikels gepostet hat. Zweifelsfrei war, dass der Online-Artikel als solches unter das in § 9 Abs. 1 DSG normierte Medienprivileg fällt. Mit Bezug auf die Judikatur des EuGH wurde ausgesprochen, dass, um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, Begriffe wie Journalismus weit ausgelegt werden müssen. Vor diesem Hintergrund muss das Privileg nach § 9 Abs. 1 DSG nach unionsrechtlichem Verständnis betrachtet werden und kann auch „Bürgerjournalismus" umfassen (wie etwa Internet-Diskussionsforen unterhalb eines journalistischen Artikels). Insbesondere war zu berücksichtigen, dass gegenständlich mit den Beiträgen der betroffenen Person auch Beiträge anderer Benutzer (in Form von Antworten oder „Diskussionsbäumen") verkettet waren. Darüber hinaus wurde das Forum im gegenständlichen Fall von der Beschwerdegegnerin als Medienunternehmen betrieben. Die Beschwerde war daher im Ergebnis zurückzuweisen.

**k. Bescheid vom 27.8.2018, GZ: DSB-D123.085/0003-DSB/2018 (Löschung, zulässige Dauer der Speicherung von Bewerberdaten, rechtskräftig, RIS)**

Der Beschwerdeführer hatte sich bei der Verantwortlichen, einer Ges.m.b.H., über eine Online-Datenbank um eine Stelle beworben. Später beantragte er die vollständige Löschung der Da-

ten seiner Bewerbung. Die Verantwortliche lehnte dies ab, worauf eine Beschwerde wegen Verletzung des Rechts auf Löschung eingebracht wurde. Wie schon bei der Ablehnung des Löschungsantrags brachte die Verantwortliche auch vor der Datenschutzbehörde vor, die Daten der Bewerbung mindestens sechs Monate speichern zu müssen, um einen eventuellen, binnen dieser Frist geltend zu machenden Anspruch auf Entschädigung wegen Verletzung des Gleichbehandlungsgesetzes (GlBG) abwehren zu können. Die Datenschutzbehörde erachtete diese Begründung für zutreffend. Die Notwendigkeit der Speicherung von Daten als mögliche Beweismittel gegen konkret bezeichnete Rechtsansprüche (gemäß §§ 17 und 26 GlBG) kann gemäß Art. 17 Abs. 3 lit. e DSGVO dem Löschungsrecht hier erfolgreich entgegengehalten werden. Eine Löschung ist hier daher erst nach Ablauf der entsprechenden (Präklusions-) Frist plus einem Monat (für die Zustellung einer möglichen Klage), demnach also sieben Monate nach Eingang der Bewerbung, geboten.

**l. Bescheid vom 13.9.2018, GZ: DSB-D123.070/0005-DSB/2018 (Geheimhaltung, kein Recht einer betroffenen Person auf bestimmte Datensicherheitsmaßnahmen, rechtskräftig, RIS)**

Die Beschwerdeführerin, die eine Beschwerde vor Organen der Vereinten Nationen gegen Österreich geführt hatte, verlangte vom Bundesministerium für Europa, Integration und Äußeres (Erstbeschwerdegegner) und vom Bundeskanzleramt (Zweitbeschwerdegegner), die mit dieser Beschwerde in Österreich befasst waren, die Löschung bzw. Pseudonymisierung der sie betreffenden Inhalte elektronischer Akten (ELAK) und erhob nach abschlägigen Antworten Beschwerde wegen Verletzung des Rechts auf Geheimhaltung infolge „unterlassener Datenlöschung bzw. Pseudonymisierung". Die Datenschutzbehörde hielt in ihrem Bescheid zunächst fest, dass keine Verletzung des Geheimhaltungsrechts (etwa in Form einer von der Beschwerdeführerin befürchteten Veröffentlichung von Daten aus ihrem Privatleben) erwiesen oder auch nur behauptet worden sei. Die Beschwerdeführerin hatte dazu das Argument potenzieller Hacker-Angriffe, „Datenlecks", oder absehbarer technologischer Innovationen, die ihre Identifizierung erleichtern könnten, ins Treffen geführt. Hinsichtlich einer Verletzung des Grundrechts auf Geheimhaltung durch eine „unterlassene Pseudonymisierung" sei festzuhalten, dass aus der DSGVO kein Recht abzuleiten ist, wonach eine betroffene Person spezifische Datensicherheitsmaßnahmen iSv Art. 32 DSGVO von einem Verantwortlichen verlangen könnte. Ebenso wenig könne eine betroffene Person – wie von der Beschwerdeführerin begehrt – spezifische Maßnahmen zur Datenminimierung iSv Art. 5 Abs. 1 lit. c DSGVO verlangen. Die Beschwerde wurde daher gegenüber beiden Beschwerdegegnern abgewiesen.

**m. Bescheid vom 21.9.2018, GZ: DSB-D130.092/0002-DSB/2018 (Verfahrensrecht, auch internationale Beschwerden müssen in Österreich in deutscher Amtssprache eingebracht werden, rechtskräftig, RIS)**

Der Beschwerdeführer brachte eine Eingabe in englischer Sprache bei der Datenschutzbehörde ein, aus der seine Absicht hervorgeht, gegen eine in Wien niedergelassene Ges.m.b.H. Beschwerde wegen Verletzung des Rechts auf Löschung zu erheben. Die Datenschutzbehörde trug dem Beschwerdeführer in einem Mangelbehebungsauftrag auf, die Beschwerde in deutscher Sprache vorzulegen. Weiters gab die Datenschutzbehörde den Hinweis, dass der Beschwerdeführer sich gemäß Art. 77 Abs. 1 DSGVO an die für Datenschutz zuständige Aufsichtsbehörde an seinem gewöhnlichen Aufenthaltsort oder Arbeitsplatz im Gebiet der Europäischen Union wenden und dabei eine dort zulässige Sprache gebrauchen könne. Der Beschwerdeführer antwortete mit einer englischsprachigen Eingabe aus der schlüssig der Wunsch hervorgeht, das Verfahren in Österreich in englischer Sprache zu führen. Darauf wurde die Beschwerde wegen nicht behobener Mängel bescheidmäßig zurückgewiesen. Begründet wird dies mit der ständigen Rechtsprechung des Verwaltungsgerichtshofs, wonach der Nichtgebrauch der deutschen Sprache als verfassungsmäßige Amtssprache einen zu behebenden Formmangel bildet. Art. 77

Abs. 1 DSGVO räume kein Recht auf Gebrauch der englischen Sprache vor der österreichischen Aufsichtsbehörde ein, sondern wolle durch Festlegung mehrerer alternativer Eingangsbehörden einer betroffenen Person die Möglichkeit eröffnen, sich an eine geografisch näher gelegene Aufsichtsbehörde zu wenden, deren Amtssprache ihr geläufig ist.

**n. Bescheid vom 5.10.2018, GZ: DSB-D123.204/0005-DSB/2018 (Verletzung des Rechts auf Geheimhaltung durch digitalen Türspion, nicht rechtskräftig)**

In diesem Bescheid hatte sich die Datenschutzbehörde mit der Frage zu beschäftigen, ob ein digitaler Türspion das Recht auf Geheimhaltung verletzen kann. Von der Datenschutzbehörde wurde zunächst festgehalten, dass es sich beim Betrieb eines digitalen Türspions um eine Bildaufnahme iSd § 12 Abs. 1 DSG handelt. Dabei ist der digitale Türspion eine technische Einrichtung, die geeignet ist, festzustellen, wer sich im Aufnahmebereich des Türspions befindet. Durch das elektronische/digitale Erfassen des Aufnahmebereichs vor der Tür werden Daten iSd Art. 4 Z 2 DSGVO verarbeitet. Unter Hinweis auf die Judikatur des OGH führte die Datenschutzbehörde aus, dass der verfahrensgegenständliche Türspion aufgrund der unmittelbaren Nähe der Wohnungseingangstüren den höchstpersönlichen Lebensbereich des Beschwerdeführers aufnimmt. Der höchstpersönliche Lebensbereich gemäß § 12 Abs. 4 Z 1 DSG umfasst nämlich grundsätzlich auch das Äußere einer Wohnungstür, weil dadurch das Betreten und Verlassen der Wohnung der betroffenen Person erfasst werden kann. Da keine Einwilligung des Beschwerdeführers vorlag, war die Bildaufnahme unzulässig. Gleichzeitig wurde die Datenverarbeitung durch den digitalen Türspion mit sofortiger Wirkung untersagt (gegen diesen Bescheid ist Beschwerde an das Bundesverwaltungsgericht erhoben worden).

**o. Bescheid vom 16.10.2018, GZ: DSB-D123.461/0004-DSB/2018 (DSB als Aufsichtsbehörde für Beschwerde gegen Staatsanwaltschaft zuständig, Verletzung im Recht auf Auskunft nach § 44 DSG, nicht rechtskräftig)**

Der Beschwerdeführer behauptete die Gesetzwidrigkeit (Unvollständigkeit) einer von einer Staatsanwaltschaft erteilten datenschutzrechtlichen Auskunft betreffend seine Beteiligung an verschiedenen Verfahren. Die Datenschutzbehörde ging im ergangenen Bescheid ausführlich auf die Frage ihrer Zuständigkeit für datenschutzrechtlich relevantes Handeln von Staatsanwaltschaften ein – die nach früherer Rechtslage regelmäßig verneint worden war –, die aber nunmehr zu bejahen ist. Staatsanwaltschaften sind – trotz ihrer organisatorischen Zuordnung zur Staatsfunktion Gerichtsbarkeit nach Art. 90a B-VG –weder als Gericht noch als unabhängige Justizbehörde iSd Art. 45 Abs. 2 DSRL-PJ anzusehen, da Staatsanwälte zwar Organe der ordentlichen Gerichtsbarkeit aber als solche an Weisungen der ihnen vorgesetzten Organe – und letztlich an Weisungen eines obersten Organs – gebunden sind.

Da sich die erteilte Auskunft in weiterer Folge als unzureichend erwies, wurde eine Rechtsverletzung festgestellt und die Staatsanwaltschaft angewiesen, Auskunft über personenbezogene Daten des Beschwerdeführers zu den in § 44 Abs. 1 DSG aufgezählten Informationen zu erteilen.

Die Beschwerdegegnerin hat gegen den Bescheid der Datenschutzbehörde Beschwerde an das Bundesverwaltungsgericht erhoben und darin insbesondere die Unzuständigkeit der Datenschutzbehörde eingewendet.

**p. Bescheid vom 31.10.2018, GZ: DSB-D123.076/0003-DSB/2018 (Verletzung im Recht auf Geheimhaltung durch „Cold Calling“ und Art. 14 DSGVO als subjektives Recht, rechtskräftig, RIS)**

In diesem Bescheid hatte sich die Datenschutzbehörde mit der Frage zu befassen, ob durch einen unerbetenen Werbeanruf („Cold Calling“) eine Verletzung im Recht auf Geheimhaltung möglich ist, und ob Art. 14 DSGVO unmittelbar als subjektives Recht geltend gemacht werden

kann. Konkret erhob die Beschwerdegegnerin die Telefonnummer des Beschwerdeführers auf der Webpage eines psychologischen Hilfsverbands. Dabei handelt es sich um eine gemeinnützige Organisation, die Hilfe für Menschen mit psychischen Erkrankungen, seelischen und psychosozialen Problemen anbietet. Der Beschwerdeführer scheint dort mit Foto als „Obmann" und Kontaktperson auf. In weiterer Folge hatte die Beschwerdegegnerin den Beschwerdeführer telefonisch kontaktiert und bot Produkte zum Verkauf an. Der Beschwerdeführer brachte eine Beschwerde bei der Datenschutzbehörde ein und stützte sich auf eine Verletzung von Art. 5 und Art. 7 DSGVO (sohin eine mangelnde Einwilligung).

Die Datenschutzbehörde bemerkte zunächst, dass Anrufe zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers („Unerbetene Nachrichten") nach der Bestimmung von § 107 Abs. 1 TKG 2003 (die Art. 13 der Richtlinie 2002/58/EG umsetzt) zu beurteilen und eine entsprechende Verwaltungsstrafe gemäß § 109 Abs. 4 Z 8 TKG 2003 ggf. von der zuständigen Fernmeldebehörde zu verhängen ist. Weiters wurde festgehalten, dass insofern eine Beurteilung der Rechtmäßigkeit der Verarbeitung iSv Art. 6 DSGVO ausgeschlossen ist. Jedoch kann durch einen Verstoß gegen das TKG 2003 gleichzeitig sehr wohl eine Verletzung des Rechts auf Geheimhaltung nach § 1 Abs. 1 DSG und auch eine Verletzung jener Bestimmungen der DSGVO vorliegen, die dem Verantwortlichen gerade keine zusätzlichen Pflichten iSv Art. 95 DSGVO auferlegen. Nach der Rechtsprechung der Datenschutzbehörde kann sich eine betroffene Person dem Grunde nach auf jede Bestimmung – auch abseits der Betroffenenrechte in Kapitel III – stützen, sofern dieser Verstoß zu einer Verletzung des Rechts auf Geheimhaltung gemäß § 1 Abs. 1 DSG führt.

Im vorliegenden Fall verwies die Datenschutzbehörde darauf, dass die Telefonnummer des Beschwerdeführers zwar auf der Webpage veröffentlicht wurde, jedoch die generelle Annahme des Nichtvorliegens einer Verletzung schutzwürdiger Geheimhaltungsinteressen für zulässigerweise veröffentlichte Daten mit den Bestimmungen der DSGVO nicht vereinbar ist. Eine auf einer Webpage veröffentlichte Telefonnummer des Beschwerdeführers, die dazu dient, als „Beratungshotline" für bedürftige Personen in Anspruch genommen zu werden, ist jedenfalls nicht als Einwilligung iSv § 107 Abs. 1 TKG 2003 zu sehen. Die Beschwerdegegnerin hat daher die Telefonnummer des Beschwerdeführers zweckwidrig für Werbemaßnahmen verwendet, weshalb eine Verletzung im Recht auf Geheimhaltung festzustellen war.

Darüber hinaus musste geklärt werden, ob eine Verletzung im Recht auf Art. 14 DSGVO vorliegt. Der Beschwerdeführer fragte im Rahmen des telefonischen Gesprächs, aus welcher Quelle die Beschwerdegegnerin die Telefonnummer habe. Die Beschwerdegegnerin teilte diese Information allerdings nicht mit. Die Datenschutzbehörde kam zu dem Ergebnis, dass die Informationspflichten gemäß Art. 14 DSGVO in Kapitel III (also den Betroffenenrechten) geregelt sind, und dass es zwar einerseits eine Pflicht des Verantwortlichen ist, gewisse Informationen bereitzustellen, dies jedoch umgekehrt auch ein Recht der betroffenen Person beinhaltet, gewisse Informationen antragsunabhängig zu erhalten. Der Beschwerdegegnerin war daher innerhalb einer Frist von zwei Wochen aufzutragen, eine vollständige Mitteilung gemäß Art. 14 DSGVO hinsichtlich jener Informationen, die dem Beschwerdeführer nicht bereits im Rahmen dieses Verfahrens zur Kenntnis gebracht wurden, zu erteilen.

**q. Bescheid vom 15.11.2018, GZ: DSB-D122.944/0007-DSB/2018 (Kein Recht auf Löschung von Krankenstandstagen und eines Aktenvermerks durch den ehemaligen Dienstgeber, rechtskräftig)**

In diesem Bescheid hatte sich die Datenschutzbehörde mit der Frage zu beschäftigen, ob der Beschwerdeführer von seinem ehemaligen Dienstgeber einerseits die Löschung seiner Krankenstandstage, welche während seines Dienstverhältnisses anfielen, und andererseits die Lö-

schung eines Aktenvermerkes, dass einer Wiedereinstellung des Beschwerdeführers nicht zugestimmt werde, begehren kann. Der Beschwerdegegner brachte hierzu vor, dass eine Löschung der Krankenstandstage aufgrund von sozialversicherungsrechtlichen- und steuerrechtlichen Aufbewahrungspflichten nicht erfolgen könne. In Bezug auf den verfahrensgegenständlichen Aktenvermerk habe ein Dienstgeber ein überwiegendes berechtigtes Interesse für sich selbst zu bestimmen, mit wem er ein Dienstverhältnis eingehe und werde der Aktenvermerk zudem als Bestandteil des Personalaktes automatisch nach drei Jahren, ab Ausscheiden des Beschwerdeführers, gelöscht. Hinsichtlich der Krankenstandstage hielt die Datenschutzbehörde fest, dass sowohl § 132 BAO als auch § 42 Abs. 1 ASVG eine rechtliche Verpflichtung im Sinne des Art. 17 Abs. 3 lit. b DSGVO zur Aufbewahrung normieren und eine Löschung daher erst nach sieben Jahren erfolgen muss. Betreffend den Aktenvermerk liegt ebenso keine unrechtmäßige Verarbeitung nach Art. 17 Abs. 1 lit. d DSGVO vor, weil der Beschwerdegegner aufgrund seines Dokumentationsinteresses ein berechtigtes Interesse gemäß Art. 6 Abs. 1 lit. f DSGVO vorweist, welches die Interessen des Beschwerdeführers überwiegt. Da der Aktenvermerk zudem mit Ablauf von drei Jahren nach Beendigung des Dienstverhältnisses, entsprechend der Verjährungsfrist des ABGB, gelöscht wird, ist die Aufbewahrungsdauer auch nicht als unverhältnismäßig anzusehen, womit im Ergebnis keine Verletzung des Beschwerdeführers im Recht auf Löschung gegeben ist.

**r. Bescheid vom 22.11.2018, GZ: DSB-D122.956/0007-DSB/2018 (keine Rechtsgrundlage für intelligente Wasserzähler, nicht rechtskräftig)**

In dieser Sache hatte sich die Datenschutzbehörde mit der Zulässigkeit eines intelligenten Wasserzählers („Smart Meters“) zu befassen, der kontinuierlich Wasserdurchfluss und Wassertemperatur erfasst und diese Daten täglich in Form von Mindest-, Mittel- und Höchstwerten für einen Zeitraum von bis zu zehn Jahren speichert. Der Beschwerdeführer machte sein Recht auf Geheimhaltung geltend und führte unter anderem aus, dass für den Verbau von intelligenten Funkwasserzählern weder eine sachliche Rechtfertigung noch eine Rechtsgrundlage vorliege und der Beschwerdegegner daher einen solchen Wasserzähler, trotz ausdrücklichem Widerspruchs des Beschwerdeführers, unrechtmäßig installiert hätte. Der Beschwerdegegner, ein Wasserverband, stützte sich hingegen bei dem Erfassen und Verwalten von Zählerdaten auf die Rechtsgrundlagen des Art. 6 Abs. 1 lit. b, e und f DSGVO und brachte unter anderem vor, dass auch bereits im Elektrizitätssektor intelligente Messgeräte vorgesehen seien und die hierfür geltenden Bestimmungen sinngemäß Anwendung finden würden.

Die Datenschutzbehörde gab der Beschwerde statt und hielt fest, dass Eingriffe durch den Beschwerdegegner gemäß § 1 Abs. 2 DSG stets einer gesetzlichen Grundlage bedürfen, da dieser als Körperschaft öffentlichen Rechts konstituiert ist und daher als staatliche Behörde nach leg. cit. qualifiziert wird. Eine Berufung auf die Rechtmäßigkeit der Verarbeitung aufgrund von Art. 6 Abs. 1 lit. b und f DSGVO ist somit nicht zulässig. Das Maß- und Eichgesetz, die Trinkwasserverordnung oder das Wasserrechtsgesetz 1959 sehen jedoch keine entsprechende gesetzliche Grundlage für den Einsatz von intelligenten Wasserzählern vor, wie dies etwa für den Elektrizitätssektor in § 16a Elektrizitätswirtschafts- und -organisationsgesetz (ElWOG) geregelt ist. Der Einbau und Betrieb des intelligenten Wasserzählers durch den Beschwerdegegner stellt daher einen unzulässigen Eingriff dar und verstößt gegen das Recht des Beschwerdeführers auf Geheimhaltung nach § 1 DSG. Der Beschwerdegegner erhob gegen den Bescheid der Datenschutzbehörde Beschwerde an das Bundesverwaltungsgericht.

**s. Bescheid vom 28.11.2018, GZ: DSB-D123.800/0001-DSB/2018 (Unzuständigkeit der Datenschutzbehörde für Beschwerde gegen das Parlament wegen veröffentlichter Protokolle eines parlamentarischen Untersuchungsausschusses, rechtskräftig)**

Der Beschwerdeführer wandte sich gegen „das Österreichische Parlament, Untersuchungsausschuss des Nationalrates“ wegen Verletzung seiner Rechte auf Geheimhaltung und Löschung

und brachte vor, er habe im Hypo-Untersuchungsausschuss des Nationalrats ausgesagt, die entsprechenden Protokolle seien immer noch, trotz seines Antrags auf Löschung, öffentlich zugänglich, die Löschung sei abgelehnt worden.

Die Datenschutzbehörde hat diese Beschwerde von Amts wegen ohne nähere Ermittlungen wegen Unzuständigkeit zurückgewiesen. Die Datenschutzbehörde ist eine Verwaltungsbehörde. Auch wenn die DSGVO die Aufsicht der Datenschutz-Aufsichtsbehörden über Organe der Gesetzgebung – anders als über Gerichte im Rahmen der justiziellen Tätigkeit (Art. 55 Abs. 3) – nicht schlichtweg verneint, so ist der europäischen Rechtsordnung die Trennung der Staatsgewalten inhärent. Eine Kontrolle der Gesetzgebung (Legislative) durch die Verwaltung (Exekutive) ist ausgeschlossen. Untersuchungsausschüsse und protokollarische Aufzeichnungen über deren Beweiserhebungen sind Aufgaben der legislativen Kontrolle über die Verwaltung und unterliegen folglich nicht der Jurisdiktionskompetenz der Datenschutzbehörde.

**t. Bescheid vom 30.11.2018, GZ: DSB-D122.931/0003-DSB/2018 (Freiwilligkeit der Einwilligung zur Setzung von Cookies gegen Zugang zu einer Online-Zeitung, rechtskräftig, RIS, Newsletter 1/2019, Seite 2)**

In diesem Bescheid, hatte sich die Datenschutzbehörde unter anderem mit der Frage zu beschäftigen, ob es den Anforderungen an die Freiwilligkeit einer Einwilligung entspricht, wenn bei Besuch der Webpage der Beschwerdegegnerin, die eine Online-Plattform inklusive Online-Zeitung betreibt, zur Setzung von Cookies eine Einwilligung eingeholt wird und dafür im Gegenzug der Zugang zu dieser Webpage gewährt wird.

Es wurde zunächst festgehalten, dass sich der Beschwerdeführer entsprechend der bisherigen Judikatur der Datenschutzbehörde auch auf jede andere Bestimmung abseits von Kapitel III DSGVO (welches die Betroffenenrechte taxativ aufzählt) stützen kann - so auch eine behauptete unfreiwillige Einwilligung -, sofern dadurch denkmöglich eine Verletzung des Rechts auf Geheimhaltung nach § 1 Abs. 1 DSG begründet wird. Darüber hinaus wurde ausgesprochen, dass Bestimmungen der Richtlinie 2002/58/EG (ePrivacy-RL) bzw. des TKG 2003 der DSGVO jeweils als lex specialis vorgehen. Die Frage der Rechtsgrundlage bzw. der Erlaubnistatbestand zur Setzung von Cookies richtet sich daher nach § 96 Abs. 3 TKG 2003, wonach eine Ermittlung von Daten (bzw. der Einsatz von „Werbe-Cookies“) nur zulässig ist, soweit eine Einwilligung erteilt wurde. Gleichzeitig verweist die Richtlinie 2002/58/EG hinsichtlich der näheren Bedingungen zu dieser Freiwilligkeit auf die seit Geltung der DSGVO nicht mehr anzuwendende Richtlinie 95/46/EG (Datenschutz-RL). In systematischer Auslegung sind daher nunmehr für die Beurteilung des Vorliegens einer freiwilligen Einwilligung die Bestimmungen der DSGVO heranzuziehen.

Die Datenschutzbehörde überprüfte den gegenständlichen Sachverhalt und berücksichtigte dabei den Umstand, dass die Beschwerdegegnerin als Alternativzugang ein Bezahlabonnement gegen geringfügiges Entgelt anbietet. Insbesondere wurde die Frage überprüft, ob die Abgabe einer Einwilligung durch den Beschwerdeführer mit beträchtlichen negativen Folgen behaftet ist, oder ob eine echte bzw. freie Wahlmöglichkeit besteht. Im Ergebnis wurde die Beschwerde abgewiesen, da als Konsequenz bei Nichtabgabe der Einwilligung entweder auf das angebotene Bezahlabonnement oder auf die physisch erscheinende Zeitung der Beschwerdegegnerin zurückgegriffen werden kann. Darüber hinaus war im vorliegenden Sachverhalt zu berücksichtigen, dass dem Beschwerdeführer bei Abgabe einer Einwilligung auch ein deutlich erkennbarer Vorteil entsteht – nämlich der Erhalt des vollen Zugangs zu einer Webpage mit journalistischen Online-Artikeln und einem moderierten Forum. Es ist somit nicht von einem absoluten Koppelungsverbot auszugehen. Das Grundrecht auf Datenschutz kann nämlich nicht nur als Abwehrrecht verstanden werden, sondern beinhaltet im Sinne der informationellen Selbstbe-

stimmung auch – selbstverständlich in gewissen Grenzen - die Hoheit über die eigenen Daten. Diese Datenhoheit muss sich jedoch nicht nur in der Ausübung der Betroffenenrechte äußern, sondern kann auch in Form der Abgabe einer Einwilligung gegen einen deutlich erkennbaren Vorteil genutzt werden, wobei die Grenzziehung immer eine Einzelfallbeurteilung ist.

**u. Bescheid vom 30.11.2018, GZ: DSB-D122.954/0010-DSB/2018 (Löschung aufgrund fehlender Information nach Art. 14 DSGVO, nicht rechtskräftig)**

In diesem Bescheid hatte sich die Datenschutzbehörde mit der Löschung personenbezogener Daten im Zusammenhang mit den Informationspflichten eines Verantwortlichen zu befassen. Der Beschwerdeführer verlangte von der Beschwerdegegnerin, einer Tochtergesellschaft eines Gläubigerschutzverbandes, die Löschung seiner Einträge in der Konsumenten- und Warenkreditevidenz. Hierbei handelte es sich in beiden Fällen um Einträge, welche dasselbe Insolvenzverfahren betreffen. In der Konsumentenkreditevidenz war jedoch die Nichteröffnung, in der Warenkreditevidenz die Erledigung des Insolvenzverfahrens vermerkt. Der Beschwerdeführer brachte vor, dass die Beschwerdegegnerin ihn über diese Einträge nicht informiert hatte, und die Gläubigerforderung darüber hinaus bereits zur Gänze beglichen worden war. Die Datenschutzbehörde gab der Beschwerde statt und hielt fest, dass aufgrund des in Art. 5 Abs. 1 lit. a DSGVO verankerten Grundsatzes von Treu und Glauben eine entsprechende Benachrichtigung des Beschwerdeführers gemäß Art. 14 DSGVO erforderlich ist. Mangels einer solchen sind die Gläubigerschutzinteressen, auf welche sich die Beschwerdegegnerin stützte, nicht mehr gerechtfertigt und erfolgten die Einträge somit rechtswidrig. Überdies hielt die Datenschutzbehörde fest, dass Voraussetzung für die Rechtmäßigkeit einer Eintragung auch die Richtigkeit der eingetragenen Information ist. Der verfahrensgegenständliche Eintrag in der Konsumentenkreditevidenz erweckte jedoch den Eindruck, dass ein Insolvenzverfahren eröffnet und abgeschlossen worden war, was nicht zutraf, da ein solches mangels kostendeckendem Vermögen erst gar nicht eröffnet wurde. Der Eintrag war daher auch aus diesem Grund zu löschen. Die Beschwerdegegnerin erhob gegen den Bescheid der Datenschutzbehörde Beschwerde an das Bundesverwaltungsgericht.

**v. Bescheid vom 5.12.2018, GZ: DSB-D123.211/0004-DSB/2018 (Recht auf partiellen Löschungsantrag, nicht rechtskräftig)**

In diesem Bescheid hatte die Datenschutzbehörde im Zuge eines Beschwerdeverfahrens die Frage zu klären, ob der Beschwerdeführer dadurch in seinen Rechten auf Geheimhaltung und Löschung verletzt wurde, weil die Beschwerdegegnerin, ein Wirtschaftsauskunftsdienst, dem partiellen Löschungsantrag des Beschwerdeführers nicht entsprochen hat. Darüber hinaus war die Frage zu klären, ob durch die Weigerung der Wiederherstellung von Daten, der Beschwerdeführer in seinem Recht auf Berichtigung verletzt wird. Dazu stellte die Datenschutzbehörde fest, dass dem Betroffenen bei einem antragsbezogenen Recht, wie jenem auf Löschung (verfahrensgegenständlich war die alte Rechtslage, somit § 27 Abs. 1 Z 2 DSG 2000 anzuwenden) freistehen muss, als „Minus“ auch die Löschung bloß eines Teiles der Daten zu begehren (partielles Löschungsrecht). Ist ein Auftraggeber/Verantwortlicher der Ansicht, dass einem partiellen Löschungsbegehren nicht entsprochen werden kann, so sind die dafür maßgeblichen Gründe – innerhalb der hiefür vorgesehen Frist – dem Betroffenen mitzuteilen, und zwar in einer Art und Weise, dass für den Betroffenen selbst, jedoch auch für die Datenschutzbehörde nachvollziehbar ist, weshalb dem Begehren nicht (vollständig) entsprochen wurde. Die Datenschutzbehörde sprach aus, dass die Vorgehensweise der Beschwerdegegnerin, die gesamten personenbezogenen Daten des Beschwerdeführers - trotz partiellen Löschungsantrages - zu löschen, nicht der Verwendung von Daten nach Treu und Glaube entspricht. Durch die verfahrensgegenständliche Löschung des gesamten Datensatzes, wurde die Integrität des Datensatzes nachhaltig beeinträchtigt, was eine Verletzung im Recht auf Geheimhaltung nach § 1 Abs. 1 DSG 2000 nach sich zieht. Darüber hinaus wurde der Beschwerdeführer durch die überschießende Löschung auch

in seinem Recht auf Löschung nach § 1 Abs. 3 Z 2 iVm § 27 DSG 2000 verletzt. In Bezug auf das Recht auf Berichtigung führte die Datenschutzbehörde schließlich aus, dass aufgrund der – unbestrittenen – gänzlichen Löschung der Daten des Beschwerdeführers eine Berichtigung (auch mittels Zusatzerklärung) oder Wiederherstellung derselben schon dem Wesen nach nicht möglich ist, weil für eine Berichtigung das faktische Vorhandensein eines zu berichtigenden Datensatzes Voraussetzung ist. Folglich war die Beschwerde in diesem Punkt abzuweisen und es war kein Leistungsauftrag zu erteilen (gegen diesen Bescheid ist Beschwerde an das Bundesverwaltungsgericht erhoben worden).

**w. Bescheid vom 5.12.2018, GZ: DSB-D123.270/0009-DSB/2018 (Entfernung des Personenbezugs („Anonymisierung") als Mittel zur Löschung, rechtskräftig, RIS)**

Im Rahmen dieses Beschwerdeverfahrens hatte sich die Datenschutzbehörde mit der Frage zu befassen, welche Mittel zur Löschung eingesetzt werden können. Der Beschwerdeführer hatte die Löschung sämtlicher Daten begehrt. Die Beschwerdegegnerin entsprach dem Löschbegehren jedoch in der Form, dass sie die Daten des Beschwerdeführers teils faktisch durch Entfernung in ihrem System gelöscht hat, teils hat sie jedoch bloß den Personenbezug zum Beschwerdeführer entfernt (also den Datenbestand des Beschwerdeführers „anonymisiert"). Der Beschwerdeführer brachte im Zuge seiner Beschwerde an die Datenschutzbehörde vor, dass das Primat der faktischen Löschung gelte, und er daher in seinem Recht auf Löschung verletzt sei.

Die Datenschutzbehörde hat festgehalten, dass dem Verantwortlichen hinsichtlich der Mittel - also der vorgenommenen Art und Weise, wie eine Löschung durchgeführt wird - ein Auswahlermessen zusteht. Da die DSGVO auf Daten ohne Personenbezug keine Anwendung findet, ist die Entfernung des Personenbezugs (also die „Anonymisierung") grundsätzlich ein mögliches Mittel, um einem Löschbegehren zu entsprechen. Dabei gilt jedoch ein strenger Maßstab, wonach sichergestellt sein muss, dass weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismäßigen Aufwand den Personenbezug wiederherstellen kann.

Die Beschwerdegegnerin hat im gegenständlichen Fall durch mehrere Screenshots von ihrem System belegt, dass der Personenbezug entfernt wurde. Darüber hinaus hat die Beschwerdegegnerin den Prozess der Entfernung des Personenbezugs ausreichend und nachvollziehbar dargelegt. Die Beschwerde wurde daher im Ergebnis abgewiesen.

**x. Bescheid vom 7.12.2018, GZ: DSB-D123.193/0003-DSB/2018 (Löschung von Bonitätsdaten durch Wirtschaftsauskunftsdienst, keine pauschale siebenjährige Speicherdauer, nicht rechtskräftig)**

Die Beschwerdeführerin wandte sich gegen eine Gesellschaft m.b.H. als Beschwerdegegnerin, die u.a. das Gewerbe der „Auskunftei über Kreditverhältnisse" (§ 152 GewO 1994) ausübt und eine Identitäts- und Bonitätsdatenbank betreibt. Sie gab an, ihre Schulden in einem Insolvenzverfahren (Zahlungsplan) getilgt zu haben. Die Beschwerdegegnerin verarbeite jedoch weiterhin „Zahlungserfahrungsdaten" (betreffend Einbringungsversuche durch Inkassobüros) über sie und habe sich geweigert, diese Daten zu löschen.

Das Ermittlungsverfahren ergab, dass die Beschwerdegegnerin, neben im Dezember 2018 noch öffentlich zugänglichen Daten aus dem Jahr 2013 des die Beschwerdeführerin betreffenden Insolvenzverfahrens aus der Ediktsdatei der Justiz, auch Daten zu zwei außergerichtlichen Inkassofällen speicherte.

Rechtlich hielt die Datenschutzbehörde fest, dass ein Wirtschaftsauskunftsdienst zur Verarbeitung von Bonitätsdaten nicht die Einwilligung der betroffenen Person benötigt, sondern sich grundsätzlich auf das überwiegende berechtigte Interesse eines zur Ausübung des Gewerbes

berechtigten Verantwortlichen stützen kann. Aus dem Gesetz ergebe sich kein einheitlicher Maßstab für die Speicherdauer von Bonitätsdaten. Diese müsse daher im Einzelfall bestimmt werden. Eine generelle Löschung der bonitätsrelevanten Daten erst sieben Jahre nach Tilgung der Schuld wird im Hinblick auf Art. 6 Abs. 1 lit. f DSGVO, vor allem aber im Hinblick auf die seit dem Zeitpunkt der Erlassung des Bescheides der Datenschutzkommission (K600.033 018/0002-DVR/2007 aus einem Registrierungsverfahren), auf den sich die Beschwerdeführerin berufen hatte, geänderte Rechtslage jedenfalls nicht verhältnismäßig sein. Die Datenschutzbehörde ging in dieser Frage ausdrücklich von der bisherigen Rechtsprechung ab.

Die Datenschutzbehörde trug in weiterer Folge dem Wirtschaftsauskunftsdienst auf, jene Bonitätsdaten zu löschen, die eine Inkassoforderung betrafen, die bereits vor Eröffnung des Insolvenzverfahrens getilgt worden war. Die Löschung von Daten zu einer Forderung, die erst im Insolvenzverfahren getilgt wurde, war dagegen nicht geboten, da die gesetzliche Frist zur Löschung dieses Verfahrens aus der Insolvenzdatei noch nicht abgelaufen war. Gegen diesen Bescheid hat die Beschwerdegegnerin Beschwerde an das Bundesverwaltungsgericht erhoben.

**y. Bescheid vom 20.11.2018, GZ: DSB-D122.895/0005-DSB/2018 (Berichtigung bzw. Vervollständigung des Inhalts eines elektronischen Personalakts, rechtskräftig, RIS)**

In dieser Sache hatte sich die Datenschutzbehörde erstmals mit dem Recht auf Berichtigung von Daten gemäß Art. 16 DSGVO zu befassen. Die Beschwerdeführerin, eine Vertragsbedienstete der Finanzverwaltung, war irrtümlich in den Verdacht geraten, eine Dienstpflichtverletzung (fehlende Krankenstandsbescheinigung) begangen zu haben. Die Kündigung ihres Dienstverhältnisses war intern in die Wege geleitet, nach Aufklärung des Sachverhaltes aber nicht ausgesprochen worden. Die Beschwerdeführerin verlangte die Berichtigung bzw. Vervollständigung ihres ausschließlich elektronisch geführten Personalaktes dahingehend, dass ausdrücklich festzuhalten sei, dass die Beschwerdeführerin keine Dienstpflichtverletzung gesetzt hätte.

Die Datenschutzbehörde stellte im Ermittlungsverfahren fest, dass die Ereignisse rund um die fehlende Krankenstandsbestätigung und das eingeleitete Kündigungsverfahren im Personalakt vollständig dokumentiert waren.

Unter Verweis auf die weiterhin zutreffende Rechtsprechung der Datenschutzkommission hielt die Datenschutzbehörde rechtlich fest, dass Daten, die für Zwecke eines behördlichen Verfahrens verwendet werden, aus datenschutzrechtlicher Sicht als richtig gelten, wenn sie das entsprechende Verfahrensergebnis formell richtig wiedergeben. Auf die inhaltliche Wahrheit der Angaben (etwa bei einer Zeugenaussage), den Wert eines Beweismittels oder dessen Zulässigkeit im Verfahren vor der als Verantwortliche tätig werdenden Behörde kommt es, vorbehaltlich ausdrücklich anderslautender gesetzlicher Regelungen, in diesem Zusammenhang hingegen nicht an. Die Beschwerdeführerin hatte kein Recht auf Berichtigung dahingehend, dass Angaben, die für sie subjektiv von Bedeutung sind, in die Dokumentation aufgenommen werden oder bestimmte Formulierungen von ihr vorgegeben werden.

Da aus der vorliegenden Dokumentation der Ereignisse nur der Schluss gezogen werden konnte, dass die Beschwerdeführerin keine Dienstpflichtverletzung begangen hatte (Informationen nicht lückenhaft oder objektiv missverständlich), wurde die Beschwerde abgewiesen.

#### 3.2.1.2 Grenzüberschreitende Fälle der DSB

Seit dem 25. Mai 2018 führt die DSB nicht nur nationale Verfahren, sondern behandelt auch grenzüberschreitende Fälle. Diese umfassen sowohl von Betroffenen erhobene Beschwerden und amtswegige Prüfverfahren, als auch Mitteilungen über Sicherheitsverletzungen gemäß Art. 33 DSGVO.

Ein grenzüberschreitender Sachverhalt liegt gemäß Art. 4 Z 23 iVm Art. 56 DSGVO dann vor, wenn eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in mehr als einem Mitgliedstaat der EU erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder eine Verarbeitung personenbezogener Daten zwar im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, diese jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.

Ergibt sich aus einer bei der DSB eingebrachten Beschwerde eine solche grenzüberschreitende Verarbeitung, weil etwa der Verantwortliche oder der Auftragsverarbeiter in einem anderen Mitgliedsstaat niedergelassen ist, dann ist in der Regel ein sog. One-Stop-Shop Verfahren gemäß Art. 56 DSGVO in Verbindung mit Art. 60 DSGVO zu führen.

Am Beginn eines solchen Verfahrens steht die Ermittlung der federführenden und betroffenen Aufsichtsbehörden für die grenzüberschreitende Verarbeitung. Die federführende Aufsichtsbehörde ist gemäß Art. 56 Abs. 1 DSGVO die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters. Als betroffene Aufsichtsbehörden sind gemäß Art. 4 Z 23 jene Aufsichtsbehörden zu bezeichnen, in deren Hoheitsgebiet der Verantwortliche oder der Auftragsverarbeiter niedergelassen ist (lit. a), wenn die grenzüberschreitende Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann (lit. b) oder eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde (lit. c).

Wurde eine grenzüberschreitende Beschwerde bei der österreichischen DSB eingebracht, deklariert sich die DSB daher im Sinne des Art. 4 Z 23 lit. c DSGVO als betroffene Behörde und nimmt als solche am One-Stop-Shop Verfahren teil. Ergibt sich aus den Ermittlungen im nationalen Verfahren, dass die DSB federführende Datenschutzbehörde im Sinne des Art. 56 Abs. 1 DSGVO ist, deklariert sich die DSB als federführende Aufsichtsbehörde und führt das Ermittlungsverfahren in Österreich unter Einbeziehung der betroffenen Aufsichtsbehörden.

Ein grenzüberschreitender Sachverhalt kann an die DSB natürlich auch von einer anderen Datenschutzbehörde herangetragen werden. In einem solchen Fall prüft die Datenschutzbehörde, wie bereits oben dargelegt, unter Heranziehung der Art. 4 Z 22 und 23 DSGVO sowie Art. 56 Abs. 1 DSGVO, ob sie als federführende oder betroffene Aufsichtsbehörde in Betracht kommt. Ergibt diese Prüfung, dass die Datenschutzbehörde federführende Aufsichtsbehörde ist, führt sie das Ermittlungsverfahren gegenüber dem Verantwortlichen in Österreich im Sinne des Art. 60 DSGVO (weiter). Wird eine Betroffenheit der DSB im Sinne des Art. 4 Z 23 DSGVO festgestellt, gibt sich die DSB als solche zu erkennen und wird im weiteren Art. 60 DSGVO Verfahren von der federführenden Aufsichtsbehörde einbezogen.

Im Jahr 2018 hat die DSB 153 nationale Beschwerdefälle bearbeitet, die einen grenzüberschreitenden Sachverhalt aufwiesen. Des Weiteren hat die DSB 427 grenzüberschreitende Verfahren geführt, die an die Datenschutzbehörde von einer anderen Aufsichtsbehörde herangetragen

wurden. Dabei führt die DSB 3 Verfahren als federführende Aufsichtsbehörde gegenüber dem Verantwortlichen.

Stehen in einem grenzüberschreitenden Fall sowohl die federführende Aufsichtsbehörde, als auch die betroffenen Aufsichtsbehörden fest und wurde das Ermittlungsverfahren durch die federführende Aufsichtsbehörde geführt, bereitet diese Aufsichtsbehörde gemäß Art. 60 Abs. 3 DSGVO einen Beschlussentwurf vor, der von den betroffenen Aufsichtsbehörden begutachtet und geprüft wird. Innerhalb einer Frist von 4 Wochen können sich die betroffenen Aufsichtsbehörden mittels eines maßgeblichen und begründeten Einspruches gegen diesen Entwurf aussprechen.

Folgt die federführende Aufsichtsbehörde diesem Einspruch nicht, so leitet sie das Kohärenzverfahren gemäß Art. 63 DSGVO für die Angelegenheit ein. Schließt sich die federführende Aufsichtsbehörde dem Einspruch allerdings an, so legt sie den anderen betroffenen Aufsichtsbehörden einen überarbeiteten Beschlussentwurf vor.

Wird kein Einspruch gegen den ursprünglichen oder überarbeiteten Beschlussentwurf erhoben, liegt ein für die federführende und die betroffenen Aufsichtsbehörden bindender Beschluss vor.

2018 wurden der DSB als betroffenen Aufsichtsbehörde 6 Beschlussentwürfe vorgelegt. 2018 wurden zwei endgültige Beschlüsse getroffen. Der erste finale Beschluss betraf eine durch den Verantwortlichen zunächst nicht ordnungsgemäß vorgenommene Löschung personenbezogener Daten, die nachträglich beseitigt und auf Grund des erstmaligen Verstoßes des Verantwortlichen mit einer Verwarnung geahndet wurde. Mit dem zweiten endgültigen Beschluss wurde eine datenschutzrechtliche Verletzung der betroffenen Person insofern verneint, als die Verwendung von - in einem öffentlichen Verzeichnis verfügbaren - Daten zu Marketingzwecken auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden könne.

Die grenzüberschreitende Verfahrensführung und Zusammenarbeit gemäß Art. 56 und 60 bis 65 DSGVO wird durch eine technische Plattform unterstützt, die für die Aufsichtsbehörden vom Sekretariat des Europäischen Datenschutzausschusses betreut wird.

### 3.2.2 Kontroll- und Ombudsmannverfahren (§ 30 DSG 2000)

Beim Kontroll- und Ombudsmannverfahren gemäß § 30 DSG 2000 handelte es sich um ein Verfahren, bei dem sich jedermann (Unternehmen, Behörde, Verein, Privatperson und so weiter) wegen einer behaupteten Verletzung seiner Rechte (zum Beispiel Auskunft, Löschung, Berichtigung) oder ihn betreffender Pflichten (beispielsweise Meldung, Information) nach dem DSG 2000 mit einer Eingabe an die DSB wenden konnte. Die Durchführung eines solchen, weitestgehend formfreien Verfahrens, war (anders als beim Beschwerdeverfahren nach § 31 DSG 2000) unabhängig vom geltend gemachten Recht (Pflicht) bzw. dem angesprochenen datenschutzrechtlichen Verantwortlichen zulässig, und zwar auch dann, wenn die Datenschutzbehörde alternativ auch zur förmlichen Rechtsdurchsetzung zuständig gewesen ist. Ziel eines solchen Verfahrens nach § 30 Abs. 6 DSG 2000 war die Herbeiführung des rechtmäßigen Zustands. Dazu konnte die Datenschutzbehörde, falls erforderlich – nicht unmittelbar durchsetzbare – Empfehlungen aussprechen. Zumeist konnte im Rahmen eines solchen Verfahrens eine datenschutzrechtlich zufriedenstellende Situation aber auch ohne Einsatz dieses Mittels erreicht werden. Mit In-Kraft-Treten der DSGVO am 25. Mai 2018 wurden alle noch laufenden, in der Rechtsnatur des Kontroll- und Ombudsmannverfahrens geführten, Verfahren in ein förmliches Beschwerdeverfahren entsprechend § 24 DSG übergeführt.

Die Eingaben im Kontroll- und Ombudsmannverfahren zwischen 1. Jänner 2018 und 24. Mai 2018 beliefen sich auf 123 Fälle. Insgesamt konnten im Jahr 2018 93 Verfahren, die ursprünglich als mediatisierende Verfahren geführt wurden, abgeschlossen werden.

### 3.2.3 Rechtsauskünfte an Bürgerinnen und Bürger

Die Datenschutzbehörde stellt auf ihrer Webseite unter https://www.dsb.gv.at/fragen-und-antworten umfassende Informationen im Zusammenhang mit dem geltenden Datenschutzrecht zur Verfügung. Hierbei handelt es sich um leicht verständliche Antworten auf die relevantesten datenschutzrechtlichen Fragen. Darüber hinaus finden sich auf der Webseite der Datenschutzbehörde unter https://www.dsb.gv.at/rechte-der-betroffenen ausführliche Informationen über die Rechte der betroffenen Personen und die Zuständigkeit der Datenschutzbehörde. Zu beachten ist, dass die Datenschutzbehörde ihre Webseite im Hinblick auf die seit 25. Mai 2018 geltende Datenschutz-Grundverordnung inhaltlich angepasst hat. Es wurde auf den Leitfaden zur DSGVO, abrufbar unter https://www.dsb.gv.at/dokumente, hingewiesen, welcher laufend aktualisiert wird.

Darüber hinaus beantwortet die Datenschutzbehörde weiterhin allgemeine Anfragen zum geltenden Datenschutzrecht schriftlich. Telefonische Rechtsauskünfte werden nicht erteilt. Die Datenschutzbehörde nimmt im Rahmen der Beantwortung von Anfragen grundsätzlich keine Vorabprüfung hinsichtlich der Unzulässigkeit/Zulässigkeit einer bestimmten Datenverwendung, der Anwendung bzw. Auslegung rechtlicher Bestimmungen oder einer sonstigen inhaltlichen Anfrage vor, da jede Antwort ein entsprechendes, vom Gesetz vorgesehenes Verfahren vor der Datenschutzbehörde, präjudizieren würde.

### 3.2.4 Genehmigungen im Internationalen Datenverkehr

Das Jahr 2018 sah zwei grundsätzliche Änderungen im österreichischen Datenschutzrecht, herbeigeführt durch die Datenschutz-Grundverordnung, vor. Die erste war die Abschaffung des Datenverarbeitungsregisters, und die zweite war die weitgehende Genehmigungsfreiheit für internationalen Datenverkehr an Länder außerhalb des EWR.

Nach dem bis 24.05.2018 geltenden System gab es zwar Genehmigungsfreiheit in bestimmten Fällen (z.B.: Drittstaaten mit angemessenem Datenschutz, Zustimmung, Vertragserfüllung), aber ein beachtlicher Teil der Vorhaben erforderte eine Genehmigung der Datenschutzbehörde. In diesen Verfahren musste der Antragssteller glaubhaft machen, dass die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Dazu gab es Instrumente wie Verträge und verbindliche interne Datenschutzvorschriften der Konzerne (Binding Corporate Rules, kurz BCRs). Die Anzahl der Anträge war beträchtlich: über 300 im Jahr 2016 und noch halb so viele im Jahr 2017.

Die Datenschutz-Grundverordnung regelt die Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen in Kapitel V. Alle bisher bekannten rechtlichen Instrumente stehen zur Verfügung; es ist nur noch in ganz wenigen Fällen eine Genehmigung erforderlich. Nur noch in Art. 46 Abs. 3 DSGVO ist in bestimmten Fällen eine Genehmigung durch die zuständige Aufsichtsbehörde vorgesehen.

So wurde nach 25. Mai 2018 nur ein einziger Fall gemäß Art. 46 Abs. 3 lit. a DSGVO bei der DSB anhängig gemacht.

Auch mit der DSGVO beschäftigt der internationale Datenverkehr die Datenschutzbehörde. Die Arbeit verlagert sich aber von den zahlreichen Genehmigungsverfahren hin zur Schaffung von Binding Corporate Rules und zur Beurteilung der Angemessenheit des Datenschutzniveaus

von Empfangsländern auf europäischer Ebene. Ende 2018 waren die Arbeiten an einer solchen Angemessenheitsregelung für Japan abgeschlossen und Gespräche mit Südkorea[1] werden nur mehr geführt.

### 3.2.5 Datenverarbeitungsregister

#### Allgemeines und Ausblick

Mit dem In-Geltung-Treten der Datenschutz-Grundverordnung am 25. Mai 2018 wurde das bei der Datenschutzbehörde angesiedelte Datenverarbeitungsregister gleichsam in den Ruhestand geschickt. Die DSGVO sieht keine Meldepflicht von Datenanwendungen vor. Somit entfällt nunmehr das Einmelden von Datenanwendungen ins Register durch die Verantwortlichen und die Vorabkontrolle durch die Datenschutzbehörde. Stattdessen hat ein Verantwortlicher das Verzeichnis seiner Verarbeitungstätigkeiten gemäß Art. 30 DSGVO zu führen und gegebenenfalls Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO vorzunehmen. Bis Ende 2019 wird das Datenverarbeitungsregister ausschließlich als Archiv weitergeführt.

#### Registrierungen:

**a. „BodyCams“ (Tirol Kliniken Gmbh)**

Der Einsatzbereich sogenannter „BodyCams“ wurde unter bestimmten Voraussetzungen auch auf verschiedene Krankenhäuser in Tirol (gegenständlich war eine Meldung der Tirol Kliniken GmbH, DVR: 0654302/056) erweitert: bisher gab es registrierte BodyCams im Bereich von ÖBB-Verkehrsstationen, im Zugbegleitdienst der Ostregion der ÖBB-Personenverkehrs AG sowie im Bereich der Polizei (siehe diesbezügliche Datenschutzberichte aus den Jahren 2016 und 2017).

Der Einsatz der BodyCams in den Krankenhäusern dient dem Zweck der Dokumentation von kritischen Situationen durch Sicherheitsmitarbeiter. Der Betriebsrat hat dem Einsatz der BodyCams zugestimmt.

Neben der Betriebsvereinbarung gibt es eine Dienstanweisung, die den Sicherheitsmitarbeitern konkrete Anleitungen zum Gebrauch der BodyCams vorschreibt: insbesondere darf eine BodyCam nur zur Deeskalation kritischer Situationen in einem Anlassfall eingesetzt werden, wobei vor einer Aktivierung die betroffenen Personen von der Bilddatenverarbeitung zu informieren sind. Der Monitor der BodyCams ist in Blickrichtung der betroffenen Personen gerichtet, um auch damit einen deeskalierenden Effekt zu erzielen. Eine Aktivierung speziell in Patientenzimmern und Behandlungsräumen ist nicht zulässig.

Ein wesentlicher Aspekt bei der Kennzeichnung (dem Hinweisschild nach dem alten § 50a DSG 2000) war, dass nicht nur auf die Tatsache der Videoüberwachung (in Form eines Piktogramms oder Schriftzugs), sondern auch auf den Auftraggeber (nach der Diktion der DSGVO: Verantwortlichen) hingewiesen wird, da dieser für einen Betroffenen sonst aus der Kennzeichnung nicht ersichtlich gewesen wäre.

**b. Videoüberwachung (Landespolizeidirektion Burgenland)**

Registriert wurde die Videoüberwachung zur Durchführung der Grenzkontrolle an den Grenzübergangsstellen Deutschkreutz-Harka sowie Schachendorf-Bucsu. Als Rechtsgrundlage hierfür diente insbesondere § 12 Abs. 2 Z 1 Grenzkontrollgesetz. Voraussetzung für die Registrierung war u.a. die Zustimmung des Rechtsschutzbeauftragten des Bundesministeriums für Inneres.

1 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

**Ablehnungen:**

**a. Videoüberwachung (Betriebsareal und Verkehrsflächen eines Gewerbeparks)**

Die Eigentümerin eines großen Betriebsareals wollte die gesamte Fläche - auch Verkehrswege - unter Verwendung von Videokameras überwachen. Auf dem Areal sind verschiedene Firmen angesiedelt. Diese haben ihre Zustimmung zur Videoüberwachung erteilt. Die gemeldete Videoüberwachung wäre notwendig, da es mehrere Einbrüche im Gewerbepark gab. Durch die Videoüberwachung sollten auch die Zufahrten und Verkehrswege erfasst werden, die sich auf dem Privatgrundstück der Antragstellerin befinden. Ein Verkehrszeichen schränkte die Zufahrt mittels allgemeinen Fahrverbots ein, ausgenommen davon sind Anrainer, landwirtschaftlicher Verkehr, Linienbusse, Radfahrer und Fahrschulfahrzeuge.

Bei den zu erfassenden Örtlichkeiten handelte es sich nach Auffassung der Datenschutzbehörde unter Berücksichtigung der Judikatur des Verwaltungsgerichtshofes um Straßen mit öffentlichem Verkehr im Sinne des § 1 Abs. 1 StVO 1960.

Nach der ständigen Spruchpraxis der Datenschutzbehörde sind an öffentlichen Orten aufgrund des staatlichen Gewaltmonopols grundsätzlich nur Behörden zur Durchführung von Videoüberwachungen berechtigt. Deren Zulässigkeit richtet sich nach den Anforderungen des Sicherheitspolizeigesetzes (vgl. § 54 Abs. 6 und 7 SPG) bzw. der Straßenverkehrsordnung (vgl. § 98e StVO 1960).

Der Meldungslegerin fehlte somit eine konkrete rechtliche Befugnis zur Videoüberwachung öffentlicher Straßen, weshalb die Registrierung der gemeldeten Videoüberwachung abzulehnen war.

**b. Informationsverbundsystem (Kredit- und Finanzwirtschaft)**

Abgelehnt wurde die Registrierung eines gemeldeten Informationsverbundsystems mit der Bezeichnung „Verdachtsdatenbank der Kredit- und Finanzinstitute“. Zweck dieses Informationsverbundsystems war der Informationsaustausch zwischen verschiedenen Banken und Finanzinstituten in Österreich zur Erfüllung von Sorgfaltspflichten und im Wesentlichen zur Betrugsbekämpfung. Die Registrierung wurde abgelehnt, da die Kunden nicht nachweislich vor Vertragsabschluss in geeigneter Weise über das Informationsverbundsystem im Sinne des § 24 Abs. 1 DSG 2000 informiert wurden. Darüber hinaus fehlte auch die notwendige Information aus Anlass der konkreten Einspeisung der Daten einer betroffenen Person in das System. Diese Person hätte vor einer konkreten Eintragung in das Informationsverbundsystem informiert werden müssen. Die Teilnehmer an dem Informationsverbundsystem hätten jedoch vorgesehen, einen Betroffenen erst zwölf Wochen nach der Eintragung in das Informationsverbundsystem „Verdachtsdatenbank“ darüber zu verständigen. Diese Vorgangsweise entsprach nicht den gesetzlichen Vorgaben. Aus Sicht der Datenschutzbehörde war die Verhältnismäßigkeit des Informationsverbundsystems insgesamt nicht gegeben, weshalb die Registrierung abzulehnen war.

**c. Informationsverbundsystem (Versicherungswirtschaft)**

Abgelehnt wurde die Registrierung eines Informationsverbundsystems der österreichischen Versicherungswirtschaft im Bereich der Sachversicherung, KFZ-Versicherung, Rechtsschutzversicherung und Unfallversicherung. Zweck dieses Informationsverbundsystems war die Betrugsprävention im Zuge der Schadensfallbearbeitung durch teilnehmende Versicherungsunternehmen. Diese Meldung wies Ähnlichkeiten - jedoch auch erhebliche Unterschiede - zum registrierten Informationsverbundsystem mit der Bezeichnung „Zentrales Informationssystem der österreichischen Versicherungswirtschaft im Bereich der Kranken- und Lebensversiche-

rung“ (siehe Datenschutzbericht 2016) auf. Die Registrierung der Meldung wurde aus mehreren Gründen abgelehnt. Ein wesentlicher Punkt, der beanstandet wurde, war, dass nicht der stichhaltige Nachweis erbracht wurde, dass Betroffene vor einer konkreten Übermittlung an andere Versicherungsunternehmen informiert werden. Jedenfalls war aus Sicht der Datenschutzbehörde die Verhältnismäßigkeit des Informationsverbundsystems vor allem im Hinblick auf die Verarbeitung von Betroffenendaten ohne Vorliegen eines konkreten Verdachts und ohne Vorliegen einer ausreichenden Rechtsgrundlage, verbunden mit der großen Anzahl an potentiell Betroffenen, nicht gegeben.

### 3.2.6 Stammzahlenregisterbehörde

#### Allgemeines und Ausblick

Mit Kundmachung vom 27. Dezember 2018 in BGBl. I Nr. 104 erfolgte eine E-Government-Gesetzesnovelle, mit der durch eine Änderung des § 7 Abs. 1 leg. cit. die bisherige Zuständigkeit der Datenschutzbehörde für Angelegenheiten des Stammzahlenregisters ab 28. Dezember 2018 auf das Bundesministerium für Digitalisierung übergehen.

Es ist dies somit das letzte Mal, dass im Datenschutzbericht Agenden der Stammzahlenregisterbehörde aufscheinen.

## Zahlen und Überblick

#### Stammzahlenregister

Im Jahr 2018 wurden über 341 Millionen bereichsspezifische Personenkennzeichen (bPK) berechnet. Das entspricht einer Steigerung von über 30% im Verhältnis zum Jahr davor. Verantwortlich dafür sind vor allem die steigende Anzahl von Nutzern der elektronischen Zustellung und Meldeverpflichtungen an FinanzOnline mittels bereichsspezifischen Personenkennzeichen bezüglich der automatischen Spendenabsetzbarkeit.

#### Vollmachtenregister

2018 wurden 735 neue Vollmachten von der Stammzahlenregisterbehörde eingetragen. In Vertretung gehandelt wurde 28.893 Mal. Berufsmäßige Parteienvertreter haben das Service 1.767 Mal benutzt. Die meisten Vertretungsbefugnisse werden automatisch aus dem Firmenbuch, Vereinsregister und dem Ergänzungsregister für sonstige Betroffene übernommen.

#### Ergänzungsregister für natürliche Personen

2018 wurden 79.517 Transaktionen im Ergänzungsregister für natürliche Personen (Neuanlagen, Übernahme ins Melderegister, Änderungen, Beendigungen) durchgeführt. 48.044 davon waren Eintragungen neuer Personen in das Register. Insgesamt waren zum Stichtag 31.12.2018 278.475 Personen eingetragen. Das entspricht einer Steigerung an eingetragenen Personen von über 17% im Verhältnis zum Jahr davor.

#### Ergänzungsregister für sonstige Betroffene

Am Ende des Jahres 2018 enthielt das Register 1.566.767 aktive und 412.677 inaktive Unternehmen. 110.724 Neueintragungen und 1.005.739 Änderungen wurden vorgenommen. Das Register wurde 2.974.511 Mal über die Weboberfläche abgefragt (das entspricht einer Steigerung von über 234% im Vergleich zum Vorjahr) und 31.662.010 Mal von Behörden über die zur Verfügung gestellte Schnittstelle abgefragt.

#### Die Aufgaben und Datenanwendungen der Stammzahlenregisterbehörde

#### Erzeugung von bereichsspezifischen Personenkennzeichen

Im E-Government-System erfolgt die eindeutige Identifikation natürlicher Personen durch eine Stammzahl und davon abgeleiteten bereichsspezifischen Personenkennzeichen (bPK). Die

Stammzahl 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 Stammzahlenregisterbehörde verwaltet.

Die Stammzahlenregisterbehörde erzeugt bPK und stellt sicher, dass diese richtig eingesetzt werden. Zu diesem Zweck müssen Verantwortliche des öffentlichen Bereichs einen Antrag bei der Stammzahlenregisterbehörde auf Gestattung der Verwendung oder Ausstattung einer Datenverarbeitung 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 Zusammenführbarkeit ihrer Daten. Sichergestellt wird insbesondere, dass es trotz der eindeutigen elektronischen Identifizierung zu keiner einfachen Zusammenführbarkeit der mit bPK verknüpften Daten kommen kann, indem die bPK für verschiedene Bereiche der öffentlichen Verwaltung anders gebildet werden. Dadurch sind diese Kennzeichen in Datenverarbeitungen eines anderen Verwaltungsbereichs unbrauchbar

### Ergänzungsregister

Die Stammzahlenregisterbehörde betrieb zwei „Ergänzungsregister“, in die sich jene natürlichen Personen und sonstige rechtlich erheblich Entitäten eintragen lassen können, die in keinem der Basisregister des E-Government-Systems (Zentrales Melderegister, Firmenbuch und Vereinsregister) 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 derartiges 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 die durch Ausstellung einer Vollmacht mittels E-ID oder Handysignatur und Übertragung auf die E-ID oder Handysignatur einer anderen Person dieser die Vertretungsvollmacht eingeräumt haben. In diesem Zusammenhang weist die Stammzahlenregisterbehörde auf das vom Bundesministerium für Finanzen betriebene Unternehmensserviceportal (USP) hin, das Unternehmen eine ähnliche Funktionalität anbietet.

## Entwicklungen

### a. Legistische Entwicklungen – Novellierungen des EGovG

Im Jahr 2018 gab es zwei E-Government-Gesetz Novellen.

Mit dem Materien–Datenschutz-Anpassungsgesetz, kundgemacht am 17. Mai 2018, BGBl. I Nr. 32, wurden zahlreiche Materiengesetze (u.a. auch das E-Government-Gesetz in Art. 57 leg. cit.) an die datenschutzrechtlichen Erfordernisse der Datenschutz-Grundverordnung und des neuen DSG angepasst.

Mit Kundmachung vom 27. Dezember 2018 in BGBl. I Nr. 104 erfolgte eine weitere E-Government-Gesetzesnovelle, mit der durch eine Änderung des § 7 Abs. 1 leg. cit. die bisherige Zuständigkeit der Datenschutzbehörde für Angelegenheiten des Stammzahlenregisters ab 28. Dezember 2018 auf das Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW) übergingen.

Anträge und Anfragen zum Stammzahlenregister sind daher seit 28. Dezember 2018 an das Bundesministerium für Digitalisierung und Wirtschaftsstandort, Abteilung I/A/2, „Internationale Beziehungen und Legistik", Stubenring 1, 1030 Wien bzw. per E-Mail an die post.szrb@bmdw.gv.at zu richten.

### b. Umsetzung eIDAS Verordnung

Bereits mit der Novelle BGBl. I Nr. 121/2017 wurden gesetzliche Maßnahmen getroffen, um die sogenannte eIDAS Verordnung (Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt) im Bereich des österreichischen E-Government zu implementieren. Unter anderem legt die eIDAS Verordnung Bedingungen fest, unter denen die Mitgliedstaaten die elektronischen Identifizierungsmittel für natürliche und juristische Personen, die einem notifizierten, elektronischen Identifizierungssystem eines anderen Mitgliedstaats unterliegen, anzuerkennen haben (Näheres unter https://www.digitales.oesterreich.gv.at/eidas-verordnung).

§ 6 Abs. 5 des E-Government-Gesetzes regelt in der aktuellen Fassung dazu folgendes:
*Elektronische Identifizierungsmittel eines anderen Mitgliedstaats der Europäischen Union, die die Anforderungen des Art. 6 Abs. 1 eIDAS-VO erfüllen, können bei Verantwortlichen des öffentlichen Bereichs wie eine Bürgerkarte für Zwecke der eindeutigen Identifikation im Sinne dieses Bundesgesetzes verwendet werden. Nach Maßgabe der technischen Voraussetzungen hat diese Anerkennung spätestens sechs Monate nach der Veröffentlichung des jeweiligen elektronischen Identifizierungssystems in der Liste gemäß Art. 9 eIDAS-VO zu erfolgen. Bei der Verwendung eines solchen elektronischen Identifizierungsmittels ist für Betroffene, die weder im Melderegister noch im Ergänzungsregister eingetragen sind, ein Eintrag im Ergänzungsregister zu erzeugen. Dafür sind die Personenidentifikationsdaten des verwendeten elektronischen Identifizierungsmittels in das Ergänzungsregister einzutragen. Besteht eine Eintragung für den Betroffenen im Melderegister oder im Ergänzungsregister, sind die Personenidentifikationsdaten des verwendeten elektronischen Identifizierungsmittels in das entsprechende Register einzutragen. Die Stammzahlenregisterbehörde hat auf Antrag des Betroffenen seine Stammzahl direkt der bürgerkartentauglichen Anwendung, bei der die Verfahrenshandlung vorgenommen wird, bereitzustellen. Die Stammzahl darf durch diese nur zur Errechnung von bPK verwendet werden.*

Mit 29. September 2018 erfolgte fristgerecht die technische Inbetriebnahme der Anerkennung eines notifizierten, elektronischen Identifizierungssystems anderer Mitgliedstaaten.

### c. Migration der Stammzahlenregisterbehörde

Mit 19. Oktober 2018 ging die Novelle des E-Government-Gesetzes in Begutachtung, mit deren § 7 Abs. 1 die Aufgaben der Stammzahlenregisterbehörde im Wirkungsbereich des Bundesministeriums für Digitalisierung und Wirtschaftsstandort situiert werden sollten. Nach Abschluss

der Begutachtung und Durchsicht der Stellungnahmen, in denen es keine wesentlichen Einwände gab, wurden vorsorglich - gemeinsam mit dem Bundesministerium für Digitalisierung und Wirtschaftsstandort sowie den Dienstleistern der Stammzahlenregisterbehörde (Bundesministerium für Inneres und Statistik Austria) – allfällig durchzuführende Maßnahmen für den Fall eines Inkrafttretens der Novelle besprochen. Dies war insbesondere deshalb notwendig und sinnvoll, als das Inkrafttreten der Novelle mit dem Ablauf des Tages der Kundmachung vorgesehen war, sodass eine vorsorgliche Planung essentiell war.

Gemeinsam und in interministerieller Zusammenarbeit konnte die Herausforderung schließlich bewältigt werden und die Umstellung der Zertifikate, Webseiten und Formulare erfolgen.

### 3.2.7 Amtswegige Prüfverfahren

Die DSB hat im Jahr 2018 129 amtswegige Verfahren eingeleitet; 95 amtswegige Verfahren wurden im Berichtszeitraum abgeschlossen.

Im Gegensatz zu amtswegigen Prüfverfahren nach § 30 DSG 2000, die nur durch Empfehlung bzw. Einstellung beendet werden konnten, kann ein Prüfverfahren nach Art. 57 Abs. 1 lit. h DSGVO mit Bescheid, der auch konkrete Anordnungen enthält, die ggf. vollstreckt werden können, abgeschlossen werden.

Am 25. Mai 2018 anhängige Prüfverfahren nach § 30 DSG 2000 wurden gemäß der Übergangsbestimmung des § 69 Abs. 4 DSG als Prüfverfahren gemäß DSGVO weitergeführt und beendet.

**Ausgewählte Verfahren:**

Neben den amtswegigen Verfahren, die aufgrund anonymer Eingaben oder Eingaben durch Behörden erfolgen (überwiegend zur Überprüfung der Rechtmäßigkeit einer Videoüberwachung), führt die Datenschutzbehörde seit 2014 jährlich Schwerpunktverfahren durch. Dabei wird ein bestimmter Sektor einer eingehenden datenschutzrechtlichen Überprüfung – einschließlich Vorortuntersuchungen – unterzogen. Im Jahr 2018 wurde – bedingt durch die Umsetzung der DSGVO und den damit verbundenen generellen Anstieg an Verfahrenszahlen – allerdings kein Schwerpunktverfahren durchgeführt.

Wenn nicht anderes angeführt ist, sind sämtliche Entscheidungen im Rechtsinformationssystem des Bundes (RIS) abrufbar bzw. werden dort zeitnahe veröffentlicht, sofern keine Anfechtung der Entscheidung vor dem Bundesverwaltungsgericht erfolgte.

**D213.600**

Dieses, noch nach § 30 DSG 2000 eingeleitete, Prüfverfahren hatte die Übergabe von Patientenkarteien durch einen Kassenarzt, der in den Ruhestand treten wollte, an eine andere Kassenärztin zum Gegenstand. Die Übergabe von Patientenkarteien ist in § 51 ÄrzteG geregelt. Demnach hat der behandelnde Arzt eine ordnungsgemäße Dokumentation über Behandlungen seiner Patienten zu führen (Patientenkartei) und diese zumindest zehn Jahre aufzubewahren. Der Kassenplanstellennachfolger, sofern ein solcher nicht gegeben ist der Ordinationsstättennachfolger, hat die Dokumentation von seinem Vorgänger zu übernehmen und für die der Aufbewahrungspflicht entsprechende Dauer aufzubewahren. Er darf sie nur mit Einwilligung des betroffenen Patienten zur Erbringung ärztlicher Leistungen verwenden. Bei Auflösung der Ordinationsstätte ohne ärztlichen Nachfolger ist die Dokumentation vom bisherigen Ordinationsstätteninhaber für die der Aufbewahrungspflicht entsprechende Dauer aufzubewahren. Gleiches gilt für die Tätigkeit als Wohnsitzarzt.

Diesem Prüfverfahren lag aber der Sachverhalt zugrunde, dass die Patientenkartei weder dem Kassenplanstellen- noch dem Ordinationsstättennachfolger übergeben worden war, sondern einer sonstigen Kassenärztin und diese die Daten zur Folgebehandlung von Patienten verwendete.

Da die Übergabe an diese Kassenärztin nach Ansicht der Datenschutzbehörde nicht durch § 51 ÄrzteG gedeckt war, stellte die Datenschutzbehörde mit Bescheid vom 1. Juni 2018, GZ DSB D213.600/0001-DSB/2018, eine Rechtsverletzung fest und ordnete die Übergabe an die Kassenplanstellennachfolgerin an.

Dagegen wurde Beschwerde an das Bundesverwaltungsgericht erhoben, welches noch im Berichtszeitraum eine mündliche Verhandlung durchführte. Eine Entscheidung des Bundesverwaltungsgerichtes dazu ist im Jahr 2018 nicht ergangen.

**D213.642**
Dieses, bereits auf Basis der DSGVO eingeleitete, Prüfverfahren hatte eine mangelhafte Einwilligungserklärung im Beitrittsformular eines Vereins zum Gegenstand.

Es wurde mit Bescheid vom 31. Juli 2018, GZ DSB-D213.642/0002-DSB/2018, festgestellt, dass die Passage:

„Datenschutzrechtliche EINWILLIGUNG gemäß Art. 6 Abs 1 lit a DSGVO zu Marketingzwecken: Ich willige ein, dass der [Verein] meine personenbezogenen Daten (Vorname, Familienname, Clubkartennummer, Adresse, Telefonnummer, E-Mail-Adresse) zum Zweck der Zusendung/ Mitteilung von Informationen über neue Angebote, Produkte und Dienstleistungen wie insbesondere über [bestimmte Angebote des Vereins]

**• per Post • per elektronischem Übermittlungsweg • per Telefon**

**verarbeitet** und an die Landesvereine des [Vereins] sowie die sonstigen Gesellschaften im [Verein]-Verbund** (inkl. XY GmbH) für diese Zwecke **übermittelt**. Die Nutzung der Daten zur Erbringung der Leistungen aus Mitgliedschaft und Schutzbrief ist von dieser Einwilligung unabhängig.

**Widerruf**: Diese Einwilligungen kann ich jederzeit per E-Mail an widerruf@[verein].at oder Brief an [...] widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung nicht berührt.“

nicht den Vorgaben der DSGVO entspricht, weil sie den Eindruck vermittelt, lediglich entscheiden zu können durch welches Medium eine Person Marketing-Zusendungen erhalten möchte, nämlich per Post, per elektronischem Übermittlungsweg oder per Telefon. Zudem trug der allgemeine Aufbau des Formulars, konkret, die Platzierung der Einwilligungserklärung nach Art. 6 Abs. 1 lit. a DSGVO direkt vor der Unterschrift, welche die Anmeldung zur Mitgliedschaft bestätigt, zur weiteren Undeutlichkeit bei. Die betroffene Person könnte die optionale Einwilligung der Verarbeitung von personenbezogenen Daten zu Marketingzwecken so als zwingenden Bestandteil des Formulars verstehen und annehmen, dass für die Mitgliedschaft auch die Einwilligung zu einer solchen Verarbeitung erforderlich ist, weil die Unterschrift der betroffenen Person erst nach dieser Textpassage gesetzt wird.

Es wurde aufgetragen, die Einwilligungserklärung anzupassen. Der Bescheid ist in Rechtskraft erwachsen.

**D213.658**
Dieses, ebenfalls nach dem DSG 2000 eingeleitete und nach der DSGVO beendete, Prüfverfahren hatte die Gültigkeit einer Einwilligungserklärung im arbeitsrechtlichen Kontext zum Gegenstand. Den Arbeitnehmern wurde seitens des Arbeitgebers eine Einwilligungserklärung vorgelegt, wonach die Arbeitnehmer einwilligen, dass die Dienstfahrzeuge des Unternehmens mit einem GPS-Überwachungssystem ausgerüstet sind. Begründet wurde dies u.a. damit, dass das System zum Schutz und zur Sicherheit des Firmeneigentums diene, zur monatlichen Abrechnung mit der Leasingfirma, zur Routenplanung- und optimierung sowie zur Disposition. Ferner werde das GPS-System als Fahrtenbuch genutzt und es gebe einen Versicherungsbonus. Das GPS-System diene somit nicht zur Mitarbeiterüberwachung.

Mit Bescheid vom 8. August 2018, GZ DSB-D213.658/0002-DSB/2018, stellte die Datenschutzbehörde fest, dass die Einwilligung nicht freiwilligt erfolgte und es wurde dem Unternehmen aufgetragen, die Verarbeitung des GPS-Systems in Einklang mit der DSGVO zu bringen. Begründend wurde ausgeführt, dass eine Einwilligung im arbeitsrechtlichen Kontext zwar möglich sei, jedoch einem klar erkennbaren Vorteil des Arbeitnehmers dienen müsse. Dies sei gegenständlich nicht der Fall.

Die Datenschutzbehörde hat nicht ausgeschlossen, dass ein derartiges System ggf. auf Basis eines anderen Rechtfertigungstatbestandes, insbesondere Art. 6 Abs. 1 lit. f DSGVO, möglich sein könnte.

Dagegen wurde Beschwerde an das Bundesverwaltungsgericht erhoben und ist bei diesem anhängig. Im Berichtszeitraum erfolgte keine Entscheidung des Bundesverwaltungsgerichtes darüber.

**D213.692**
Da innerhalb eines kurzen Zeitraumes mehrere Meldungen nach Art. 33 DSGVO bei der Datenschutzbehörde einlangten, nahm die Datenschutzbehörde dies zum Anlass, ein amtswegiges Prüfverfahren nach der DSGVO gegen diesen Verantwortlichen einzuleiten.

Mit Bescheid vom 16. November 2018, GZ DSB-D213.692/0001-DSB/2018, wurden zahlreiche Rechtsverletzungen festgestellt, wie etwa

- dass entgegen den Vorgaben der DSGVO kein Datenschutzbeauftragter bestellt worden war,
- dass die verwendete Einwilligungserklärung mangelhaft war, indem eine Einwilligung für Tatbestände verlangt wurde, die keiner Einwilligung zugänglich waren (bspw. Minderung von Datensicherheitsmaßnahmen)
- dass gegen die Informationspflichten nach Art. 13 und 14 DSGVO verstoßen worden war und
- dass für bestimmte Datenverarbeitungen entgegen den Vorgaben der DSGVO keine Datenschutz-Folgenabschätzung durchgeführt worden war.

Es wurde aufgetragen, den rechtskonformen Zustand herzustellen.

Dieser (maßgebliche) Bescheid ist in Rechtskraft erwachsen, ein Verwaltungsstrafverfahren nach Art. 83 DSGVO ist anhängig.

**D213.705**
Dieses amtswegige Prüfverfahren bezog sich auf eine Staatsanwaltschaft und wurde aufgrund der Eingabe einer Anwältin eingeleitet, die behauptet hatte, in einer Strafsache einen Mandanten zu vertreten und welcher von der Staatsanwaltschaft aufgrund eines Antrages auf Akten-

übermittlung auch Aktenteile zu einem völlig anderen Verfahren (ebenfalls gegen denselben Beschuldigten) übermittelt worden waren.

Die Datenschutzbehörde hatte zunächst zu prüfen, ob sie befugt ist, ihre Aufsichtsbefugnisse gegenüber einer Staatsanwaltschaft wahrzunehmen. Gemäß der Rechtslage nach dem DSG 2000 war dies ausgeschlossen. Nach der Rechtslage seit dem 25. Mai 2018 sind von der Aufsicht durch die Datenschutzbehörde nur mehr Gerichte ausgenommen, sofern eine Datenverarbeitung „im Rahmen der justiziellen Tätigkeit“ erfolgt. Nach den Vorgaben der RL 2016/680 können die Mitgliedstaaten aber auch andere „unabhängige Justizbehörden“ von der Aufsicht ausnehmen.

Die Datenschutzbehörde kam nach Prüfung der Rechtslage zum Schluss, dass es sich bei einer österreichischen Staatsanwaltschaft – aufgrund der Weisungskette bis zu einem obersten Organ – um keine „unabhängige Justizbehörde“ handelt und bejahte ihre Zuständigkeit.

In der Sache wurde eine Rechtsverletzung infolge überschießender Datenübermittlung festgestellt (Bescheid vom 22. November 2018, GZ DSB-D213.705/0003-DSB/2018).

Der Bescheid wurde seitens der Staatsanwaltschaft bekämpft und ist vor dem Bundesverwaltungsgericht anhängig.

### 3.2.8 Äußerungen in Beschwerdeverfahren vor dem Bundesverwaltungsgericht

Im Berichtszeitraum ist die Anzahl der Beschwerdeverfahren vor dem Bundesverwaltungsgericht stark angestiegen. Mit der Datenschutz-Grundverordnung (DSGVO) traten mehrere Änderungen ein, die zu diesem Anstieg führten: Die Datenschutzbehörde wurde auch für den privaten Bereich in vollem Umfang zuständig und entscheidet seither mit Bescheiden, die beim Bundesverwaltungsgericht bekämpft werden können. Dazu kamen die neuen Rechte nach der DSGVO (Information, Einschränkung der Verarbeitung und andere), über die ebenfalls mit Bescheid entschieden wird (siehe dazu den Abschnitt zu den Individualbeschwerden).

Der Anstieg der Fälle ist stark (siehe die Statistik), aber proportional geringer als der Anstieg der Beschwerdefälle. Es muss bedacht werden, dass auch bei den Beschwerdefällen nicht jede Beschwerde zu einem Bescheid führt. Es gibt Verfahrenseinstellungen gemäß § 24 Abs. 6 DSG, falls im laufenden Verfahren erforderliche Handlungen (Auskunft, Löschung) nachgeholt wurden, und Zurückziehungen. Weiters gibt es viele Bescheide, die eine Zurückweisung wegen Nichtverbesserung von Mängeln zum Gegenstand haben (§ 13 Abs. 3 Allgemeines Verwaltungsverfahrensgesetz 1991). Diese Entscheidungen werden erfahrungsgemäß weniger bekämpft.

Es gab fünf Säumisbeschwerden im Jahr 2018. In einem dieser Fälle entschied das Bundesverwaltungsgericht, dass keine Entscheidungspflicht vorlag.

**W214 2127449-1 vom 27. September 2018**

In einer Beschwerde an das Bundesverwaltungsgericht wurde behauptet, ein Auskunftsverlangen eines Betroffenen sei per E-Mail und daher nicht schriftlich gestellt worden. Außerdem sei damit die Identität der mitbeteiligten Partei sinngemäß nicht gesetzmäßig nachgewiesen worden. Abgesehen davon, dass die belangte Behörde festgestellt hat, dass die mitbeteiligte Partei ihr Auskunftsverlangen zwar nicht als eigenhändig unterschriebene Erklärung, aber als elektronische Kopie einer solchen Erklärung in Schriftform unter Anschluss eines im Sinne der Rechtsprechung (VwGH E 9.9.2008,VwSlg 17515 A/2008) tauglichen Identitätsnachweises der Beschwerdegegnerin per E-Mail übermittelt hat, hätte die Beschwerde solche Einwände gemäß § 26 Abs. 3 DSG 2000 schon im Vorverfahren geltend machen und den Betroffenen auffordern müssen, sein

Auskunftsverlangen entsprechend zu verbessern. Dies hat sie nicht getan, stattdessen das Auskunftsverlangen beantwortet und auch im weiteren Verlauf des Verwaltungsverfahrens keine Zweifel an der Identität der Betroffenen und der Echtheit ihrer Willenserklärung geäußert. Die Datenschutzbehörde hat daher schon im angefochtenen Bescheid diesen Einwand zu Recht verworfen.

Das Bundesverwaltungsgericht verwarf diese Einwände und wies die Beschwerde gegen den Bescheid der Datenschutzbehörde ab.

**W253 2140428-1 vom 1. Oktober 2018**
Im Jahr 2016 hatte die Datenschutzbehörde die Beschwerde eines Bediensteten der Stadt Wien wegen Verletzung des Geheimhaltungsrechts abgewiesen. Dieser hatte als Personalvertreter geltend gemacht, dass eine Dienstvorgesetzte eine E-Mail unrechtmäßig an Personalvertreter, die einer anderen Gewerkschaftsfraktion angehörten, weitergeleitet hatte. Beantragt war die Feststellung der Rechtsverletzung.

Das Bundesverwaltungsgericht hat der Beschwerde gegen diesen Bescheid stattgegeben und festgestellt, dass der Beschwerdeführer durch den gerügten Verarbeitungsvorgang im Dezember 2014 im Geheimhaltungsrecht verletzt worden ist. Das Bundesverwaltungsgericht hat dabei zur Beurteilung der Rechtmäßigkeit der Verarbeitung die Bestimmungen der DSGVO, insbesondere Art. 6 Abs. 1 letzter Satz, herangezogen.

Die DSB hat dieses Erkenntnis in einer ordentlichen Revision beim Verwaltungsgerichtshof bekämpft.

Dieser Fall wurde auch im Newsletter der Datenschutzbehörde 1/2019 behandelt.

**W214 2205260-1 vom 8. Oktober 2018**
Der Beschwerdeführer hat beim Bundesverwaltungsgericht eine Maßnahmenbeschwerde gegen einen Mängelbehebungsauftrag der Datenschutzbehörde erhoben. Die Datenschutzbehörde erteilt Mängelbehebungsaufträge, wenn eine Beschwerde insb. nicht den Anforderungen des § 24 Abs. 2 und 3 DSG entspricht.

Die Beschwerde an das Bundesverwaltungsgericht wurde von diesem zurückgewiesen. Nach ständiger Rechtsprechung des VwGH kann nicht Gegenstand einer Maßnahmenbeschwerde sein, was in einem Verwaltungsverfahren geklärt werden kann. Eine Maßnahmenbeschwerde ist nach dieser Judikatur etwa dann nicht zulässig, wenn die Partei die Feststellung des strittigen Rechts mittels Bescheid begehren kann.

Im gegenständlichen Fall wird durch den Mängelbehebungsauftrag der Datenschutzbehörde im Rahmen eines Beschwerdeverfahrens vor dieser Behörde weder in subjektive Rechte des Beschwerdeführers eingegriffen, noch physischer Zwang bei Nichtbefolgung des Mängelbehebungsantrages angedroht. Daher kann mangels eines Aktes verwaltungsbehördlicher Befehls- und Zwangsgewalt schon begrifflich kein Fall einer Maßnahmenbeschwerde vorliegen. Überdies erging der Mängelbehebungsauftrag im Rahmen eines Verwaltungsverfahrens, dessen abschließender Bescheid bekämpft werden kann bzw. konnte.

### 3.2.9 Verfahren über die Meldung der Verletzung des Schutzes personenbezogener Daten

In Art. 33 DSGVO ist vorgesehen, dass Verantwortliche (Art. 4 Z 7 DSGVO) eine Verletzung des Schutzes personenbezogener Daten (sogenannter „Data Breach“) unverzüglich und möglichst binnen 72 Stunden, nachdem ihnen die Verletzung bekannt wurde, der zuständigen Datenschutzbehörde zu melden haben, außer die Verletzung des Schutzes personenbezogener Daten

führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen (Art. 34 DSGVO).

Eine Spezialbestimmung für Betreiber öffentlicher Kommunikationsdienste sieht darüber hinaus § 95a TKG vor.

**Regelungszweck**
Hintergrund der Meldung einer Verletzung des Schutzes personenbezogener Daten ist, dass diese Verletzung einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen kann, wenn nicht rechtzeitig und angemessen reagiert wird. Zu diesen Schäden gehören etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

Um sicherzustellen, dass die betroffenen Personen von der Verletzung ihrer personenbezogenen Daten erfahren, sollte die Sicherheitsverletzung wahrscheinlich zu einem hohen Risiko für diese führen, kommt der Datenschutzbehörde nach Art. 34 Abs. 4 DSGVO (bzw. vergleichbar § 95a Abs. 3 TKG) auch die Befugnis zu, vom Verantwortlichen zu verlangen, die Benachrichtigung der betroffenen Personen nachzuholen.

**Verfahren und Zahlen**
Neben den Sicherheitsverletzungen, die Verantwortliche im Inland betreffen, ist die Datenschutzbehörde mit grenzüberschreitenden Sicherheitsverletzungen (der Verantwortliche hat seinen Sitz in mehr als einem Mitgliedstaat der Union bzw. die Sicherheitsverletzung hat oder kann erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat der Union haben) konfrontiert sowie mit Sicherheitsverletzungen, die einer anderen Aufsichtsbehörde gemeldet worden sind, jedoch auch der österreichischen Datenschutzbehörde im Rahmen des Verfahrens gemäß Art. 56 DSGVO zur Kenntnis gebracht werden. Im letztgenannten Verfahren hat die Datenschutzbehörde dabei ihre Zuständigkeit als federführende oder betroffene Aufsichtsbehörde wahrzunehmen.

In Zahlen ausgedrückt wurden dabei der Datenschutzbehörde im Jahr 2018 69 Sicherheitsverletzungen gemäß § 95a TKG, sieben grenzüberschreitende Sicherheitsverletzungen, 43 Sicherheitsverletzungen ausländischer Aufsichtsbehörden sowie 501 inländische Sicherheitsverletzungen gemeldet.

**Im Berichtszeitraum erscheint folgender Fall erwähnenswert:**
Im Bescheid vom 8. August 2018, GZ: DSB-D084.133/0002-DSB/2018, hatte sich die Datenschutzbehörde mit den Voraussetzungen, unter welchen die Datenschutzbehörde von den Verantwortlichen verlangen kann, eine nach Art. 34 Abs. 1 DSGVO gebotene Benachrichtigung nachzuholen, zu befassen. Die Verantwortliche meldete der Datenschutzbehörde, dass ein Suchtmittelbuch verloren worden sei, in dem von ca. 150 Patienten in unverschlüsselter Form der Name, der körperliche Gesundheitszustand sowie die verabreichte Menge des Suchtgiftes enthalten waren. Die Verantwortliche ging im vorliegenden Fall davon aus, dass die betroffenen Patienten nicht zu benachrichtigen seien, weil kein hohes Risiko für diese vorläge. Insbesondere könnten die verarbeiteten Daten in den „falschen Händen“ eine Bloßstellung bzw. einen Identitätsdiebstahl-/betrug nur mit großem Rechercheaufwand ermöglichen. Die Datenschutzbehörde sah dies anders und trug der Verantwortlichen die Benachrichtigung der betroffenen Patienten auf. Begründet wurde dies damit, dass im Suchtgiftbuch auch

Gesundheitsdaten gemäß Art. 4 Z 15 DSGVO enthalten waren. Ein hohes Risiko für die Rechte und Freiheiten betroffene Personen besteht jedenfalls bei umfangreicher Verarbeitung besonderer Kategorien von Daten, worunter auch Gesundheitsdaten fallen. Ausnahmen der Benachrichtigungspflicht gemäß Art. 34 Abs. 3 DSGVO lagen nicht vor. Der Bescheid erwuchs in Rechtskraft.

### 3.2.10 Konsultationsverfahren

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche gemäß Art. 35 DSGVO vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Geht aus dieser Datenschutz-Folgenabschätzung nun hervor, dass, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, die beabsichtigte Verarbeitung ein hohes Risiko zur Folge hätte, hat der Verantwortliche die Aufsichtsbehörde zu konsultieren. Im Rahmen dieses Konsultationsverfahrens gemäß Art. 36 DSGVO hat die Aufsichtsbehörde nun verschiedene Befugnisse. Einerseits kann sie dem Verantwortlichen bzw. dem Auftragsverarbeiter schriftliche Empfehlungen unterbreiten, sofern sie der Ansicht ist, dass die geplante Verarbeitung nicht im Einklang mit der DSGVO steht, etwa, weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat. Darüber hinaus kann die Aufsichtsbehörde sämtliche in Art. 58 DSGVO genannten Befugnisse ausüben.

Im Jahr 2018 wurde die Datenschutzbehörde als Aufsichtsbehörde in zwei Fällen gemäß Art. 36 DSGVO konsultiert. Im ersten Konsultationsverfahren ging es um eine beabsichtigte Bildverarbeitung, und zwar die Aufnahme und kurzzeitige Speicherung von Videos mittels an der Frontscheibe eines Kfz angebrachter Videokamera („Dashcam“). Da aufgrund mehrerer Überlegungen davon auszugehen ist, dass die beabsichtigte Verarbeitung gegen die DSGVO verstoßen würde, erging neben einer Empfehlung, die beabsichtigte Verarbeitung von Daten möge nicht durchgeführt werden, auch eine Warnung gemäß Art. 58 Abs. 2 lit. a DSGVO (Empfehlung vom 9.7.2018 bzw. Bescheid vom 9.7.2018, jeweils GZ DSB-D485.000/0001-DSB/2018).

Im zweiten Antrag auf vorherige Konsultation gemäß Art. 36 DSGVO ging es um die beabsichtigte Datenverarbeitung in Form des Betriebs mehrerer Videokameras im Bereich eines Betriebsgeländes. Aus der an die Datenschutzbehörde übermittelten Datenschutz-Folgenabschätzung ging hervor, dass die identifizierten Risiken aufgrund der zu treffenden Abhilfemaßnahmen als sehr gering einschätzt worden seien, jedoch die Überwachung von Straßen des öffentlichen Verkehrs ungeachtet der getroffenen Maßnahmen generell mit einem hohen Risiko verbunden sei und daher eine vorherige Konsultation als notwendig erachtet werde. Mit Bescheid vom 18.12.2018, GZ DSB-D485.001/0003-DSB/2018, wurde der Antrag auf vorherige Konsultation zurückgewiesen und ausgesprochen, dass die Einschätzung der getroffenen Abhilfemaßnahmen allein beim Verantwortlichen liegt und eine Konsultation der Datenschutzbehörde gemäß Art. 36 DSGVO nur in jenen Fällen zur Anwendung gelangt, in denen es dem Verantwortlichen nicht gelingt, die ermittelten Risiken hinreichend einzudämmen. Da schon aus der durchgeführten Datenschutz-Folgenabschätzung hervorging, dass die Risiken aufgrund der zu treffenden Abhilfemaßnahmen als sehr gering einschätzt werden, waren die Voraussetzungen für eine vorherige Konsultation in diesem Fall nicht gegeben.

### 3.2.11 Anträge auf Genehmigung von Verhaltensregeln

**Verhaltensregeln seit 25. Mai 2018**
Das Rechtsinstrument der „Verhaltensregeln" war bereits im Datenschutzgesetz 2000 geregelt, spielte in der Praxis jedoch eine untergeordnete Rolle. Seit 25. Mai 2018 gingen bei der Datenschutzbehörde sieben Anträge auf Genehmigung von Verhaltensregeln ein, was auf ein nunmehr deutlich größeres Interesse an der Ausarbeitung von Verhaltensregeln hindeutet.

Die Datenschutzbehörde genehmigte am 19. November 2018 österreichweit die ersten Verhaltensregeln (eingereicht durch die ISPA, Internet Service Providers Austria), allerdings mit der aufschiebenden Bedingung, dass die in der DSGVO vorgesehene Überwachungsstelle in weiterer Folge auch akkreditiert wird (dazu sogleich). Vor dem Hintergrund des regen Interesses an Verhaltensregeln wird in weiterer Folge näher auf die Ausarbeitung und das Verfahren rund um die Genehmigung von Verhaltensregeln eingegangen.

**Allgemeines**
Die Systematik der Datenschutz-Grundverordnung (DSGVO) geht insgesamt von einer weitreichenden Selbstverantwortung aus und sieht mit der Schaffung von Verhaltensregeln („Codes of conduct") gemäß Art. 40 DSGVO nunmehr eine Methode zur Selbstregulierung vor, um Rechtsunsicherheiten im Zusammenhang mit der DSGVO und der Verarbeitung personenbezogener Daten innerhalb einer spezifischen Branche zu beseitigen.

Verhaltensregeln stellen Leitlinien einer guten Datenschutzpraxis dar und können die datenschutzrechtliche Verhaltensweise von Verantwortlichen und Auftragsverarbeiten einer bestimmten Branche standardisieren. Die Ausarbeitung von Verhaltensregeln soll vor allem den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen dienen.

**Antragslegitimation**
Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können einen Antrag auf Genehmigung von branchenspezifischen Verhaltensregeln bei der Datenschutzbehörde stellen. Als Antragsteller insbesondere legitimiert sind somit gesetzliche Interessenvertretungen (etwa Kammern oder Berufsverbände) oder private Verbände und Vereinigungen (etwa freiwillige Zusammenschlüsse), die bescheinigen können, dass diese eine relevante Anzahl von Verantwortlichen oder Auftragsverarbeitern vertreten.

Damit soll auch verhindert werden, dass unterschiedliche Verhaltensregeln innerhalb derselben Branche entworfen werden.

Ferner muss ausdrücklich mitgeteilt werden, ob die entworfenen Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten abzielen („internationale Verhaltensregeln") oder ob die Verhaltensregeln sich in der Erfassung von inländischen Verarbeitungstätigkeiten erschöpfen („nationale Verhaltensregeln").

Während im zweiten Fall die Datenschutzbehörde die Genehmigung von Verhaltensregeln selbst erteilen kann, muss bei einem Antrag auf Genehmigung „internationaler Verhaltensregeln" der Entwurf vor Genehmigung dem Europäischen Datenschutzausschuss vorgelegt werden.

**Inhalt**
Der mögliche Inhalt von Verhaltensregeln ist nicht abschließend vorgegeben. Nach Art. 40 Abs. 2 kann die Anwendung der DSGVO jedoch in folgenden Bereichen präzisiert werden:

a. faire und transparente Verarbeitung;
b. die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen;
c. Erhebung personenbezogener Daten;
d. Pseudonymisierung personenbezogener Daten;
e. Unterrichtung der Öffentlichkeit und der betroffenen Personen;
f. Ausübung der Rechte betroffener Personen;
g. Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist;
h. die Maßnahmen und Verfahren gemäß den Art. 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Art. 32;
i. die Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und die Benachrichtigung der betroffenen Person von solchen Verletzungen des Schutzes personenbezogener Daten;
j. die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen oder
k. außergerichtliche Verfahren und sonstige Streitbeilegungsverfahren zur Beilegung von Streitigkeiten zwischen Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung, unbeschadet der Rechte betroffener Personen gemäß den Art. 77 und 79.

Verhaltensregeln können dabei durchaus strengere Regelungen als die DSGVO selbst vorsehen, ein Unterschreiten des Datenschutzniveaus sowie die Einschränkung von Betroffenenrechten außerhalb der Vorgaben der DSGVO ist jedoch unzulässig. Dabei ist insbesondere zu berücksichtigen, dass ein Verfahren zur Genehmigung von Verhaltensregeln keine Einzelfallüberprüfung wie ein Beschwerdeverfahren zum Gegenstand hat, sondern genehmigte Verhaltensregeln generell abstrakte Wirkung besitzen.

Es ist daher nicht möglich, etwa einen bestimmten Verarbeitungsvorgang (etwa ein Geschäftsmodell) ganz allgemein für zulässig zu erklären („Die berechtigten Interessen des Verantwortlichen überwiegen“). Es muss Spielraum für eine Beurteilung im Einzelfall gelassen werden.

Darüber hinaus darf sich der Inhalt von Verhaltensregeln nicht überwiegend in der bloßen Wiedergabe der DSGVO oder des DSG erschöpfen, sondern soll im Ergebnis einen branchenspezifischen Mehrwert schaffen. Bloß allgemeine Verweise („Soweit gemäß Art. 6 DSGVO zulässig“) oder unpräzise Vorgaben („Die Speicherfristen richten sich nach der BAO“) schaffen keinen relevanten Mehrwert.

**Verfahrensregeln und Überwachungsstelle**
Ein wesentliches Kriterium von Verhaltensregeln ist die obligatorische Überwachung von Verhaltensregeln. Es müssen daher Verfahren vorgesehen sein, die es einer Überwachungsstelle („monitoring body“) ermöglichen, die Bewertung sowie die regelmäßige Überprüfung der Einhaltung von Verhaltensregeln durchzuführen. Ebenso muss die Unterwerfung unter sowie der Ausschluss von Verhaltensregeln reguliert sein.

Eine Überwachungsstelle ist eine private Stelle, die unbeschadet der Aufgaben und Befugnisse der Aufsichtsbehörde mit dieser obligatorischen Überwachung betraut wird. Zu beachten ist, dass Verfasser von Verhaltensregeln nur eine durch die Datenschutzbehörde akkreditierte Stelle als Überwachungsstelle auswählen können. Eine Überwachungsstelle muss daher zunächst einen Antrag auf Akkreditierung stellen.

Die näheren Voraussetzungen dieser Akkreditierung werden im Rahmen einer „Akkreditierungs-Verordnung“ nach Durchführen eines Begutachtungsverfahrens und nach Befassung des Europäischen Datenschutzausschusses durch die Datenschutzbehörde kundgemacht werden. Zwar kann bis dahin dennoch ein Antrag auf Genehmigung von Verhaltensregeln gestellt werden, jedoch wird eine etwaige Genehmigung nur unter der aufschiebenden Bedingung erteilt, dass die gewählte Überwachungsstelle in weiterer Folge auch akkreditiert wird.

**Wirkung der Unterwerfung**
Mit Unterwerfung unter Verhaltensregeln sind mehrere Wirkungen verbunden. So

- indiziert die Teilnahme an Verhaltensregeln etwa die Erfüllung der Pflichten eines Verantwortlichen (Art. 24 Abs. 3 und Art. 32 Abs. 3 DSGVO),
- können Verhaltensregeln „geeignete Garantien zur Datenübermittlung in ein Drittland oder an eine internationale Organisation darstellen (Art. 46 Abs. 2 lit. e DSGVO),
- sind Verhaltensregeln bei der Beurteilung der Auswirkungen eines beabsichtigten Verarbeitungsvorganges im Rahmen einer Datenschutz-Folgeabschätzung zu berücksichtigen (Art. 35 Abs. 8 DSGVO) und
- wird die Teilnahme an Verhaltensregeln bei einer etwaigen Geldbuße gebührend berücksichtigt (Art. 83 Abs. 2 lit. j).

Zu beachten ist jedoch, dass nicht jeder Angehörige einer Branche mit Genehmigung von branchenspezifischen Verhaltensregeln automatisch an diesen Verhaltensregeln teilnimmt. Eine Teilnahme ist fakultativ, weshalb sich Verantwortliche und Auftragsverarbeiter proaktiv den genehmigten Verhaltensregeln unterwerfen müssen. Nur die Unterwerfung unter genehmigte Verhaltensregeln, die durch eine akkreditierte Stelle überwacht werden, löst die oben genannten Wirkungen aus.

**Genehmigung**
Die Datenschutzbehörde genehmigt Verhaltensregeln mit Bescheid und veröffentlicht diese auf ihrer Homepage sowie im Rechtsinformationssystem (RIS).

Ein Antrag auf Genehmigung von Verhaltensregeln an die Datenschutzbehörde löst eine Gebührenpflicht aus.

### 3.2.12 Verwaltungsstrafverfahren

Mit dem In-Geltung-Treten der DSGVO und dem Inkrafttreten des DSG am 25. Mai 2018 ist die behördliche Zuständigkeit zur Führung von Verwaltungsstrafverfahren im Bereich des Datenschutzrechts von den Bezirksverwaltungsbehörden auf die Datenschutzbehörde (DSB) übergegangen. Festgelegt wird die Strafkompetenz der DSB auf Ebene des Unionsrechts in Art. 58 Abs. 2 lit. b und i iVm Art. 83 DSGVO sowie in den nationalen Begleitvorschriften der §§ 22 Abs. 5, 30 und 62 Abs. 5 DSG. Die DSB ist dabei zuständig für die Verfolgung aller Datenschutzverletzungen im gesamten Bundesgebiet.

Die Datenschutzbehörde hat von den Bezirksverwaltungsbehörden 75 zum Zeitpunkt des Zuständigkeitsüberganges anhängige Verwaltungsstrafverfahren übernommen; bedingt durch die geänderte Rechtslage war eine Vielzahl dieser Verfahren auf Grund des in § 69 Abs. 5 DSG normierten Günstigkeitsprinzips einzustellen[2]. So ist beispielsweise eine Verletzung der nach dem Regime des DSG 2000 bestehenden Meldepflicht an das Datenverarbeitungsregister (DVR) aufgrund der für den Beschuldigten neuen, günstigeren Rechtslage nicht mehr zu verfolgen.[3] Auch konn-

2 Auf grundrechtlicher Ebene ergibt sich im Anwendungsbereich des Unionsrechts das Günstigkeitsprinzip bereits aus den Gewährleistungen des Art 49 Abs. 1 GRC.
3 Vgl. hierzu nunmehr Art 30 DSGVO, der dem Verantwortlichen die Pflicht zur Führung eines Verzeichnis-

ten Beschuldigte in mehreren Fällen nachweisen, dass deren – vermeintlich auf unzulässige Weise betriebenen – Videokameras in Wirklichkeit bloße Attrappen waren.

Seit dem 25. Mai sind im Berichtszeitraum 59 Verwaltungsstrafverfahren von der DSB eingeleitet worden. Beim Großteil dieser Fälle handelt es sich um Videoüberwachungen, die (mutmaßlich) nicht den gesetzlichen Vorgaben entsprechen, weil sie etwa öffentlichen Raum oder Nachbargrundstücke erfassen und/oder nicht geeignet gekennzeichnet sind. Darüber hinaus wurden weitere Verfahren anhängig gemacht, weil Verantwortliche im Verdacht standen, gegen die in Art. 5 Abs. 1 DSGVO geregelten Grundpflichten zu verstoßen, Datenverarbeitungen vornehmen ohne sich auf einen der in Art. 6 abschließend geregelten Erlaubnistatbestände stützen zu können, die Sicherheit der Verarbeitung im Sinne des Art. 32 DSGVO nicht im ausreichenden Maße gewährleistet haben oder ihre Informationspflichten gemäß Art. 13 und 14 DSGVO nicht wahrgenommen haben. Gegenstand von Verwaltungsstrafverfahren war zudem auch das Unterlassen einer rechtzeitigen Meldung an die Datenschutzbehörde im Falle von Sicherheitsverletzungen (Art. 33 DSGVO).

Nach Art. 83 Abs. 1 DSGVO ist seitens der zuständigen Aufsichtsbehörde sicherzustellen, dass die Verhängung von Geldbußen für Verstöße gegen diese Verordnung im Einzelfall wirksam, verhältnismäßig und abschreckend ist. Gemäß Abs. 2 leg. cit. werden Geldbußen je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Art. 58 Abs. 2 lit . a bis h und j verhängt. Art. 83 Abs. 2 DSGVO zählt daran anknüpfend Kriterien auf, die bei der Entscheidung über die Verhängung einer Geldbuße und über deren Höhe in jedem Einzelfall zu berücksichtigen sind, beispielhaft genannt seien hier Kriterien wie die Art, Schwere und Dauer des Verstoßes (lit. a), Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes (lit. b), der Grad der Verantwortung unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen (lit. c) oder auch einschlägige frühere Verstöße (lit. d). Die Bestimmungen in Art. 83 DSGVO gelten grundsätzlich – der Rechtsnatur einer Verordnung entsprechend – unmittelbar und verdrängen im Anwendungsbereich des Unionsrechts die ansonsten zur Anwendung gelangenden Bestimmungen des Verwaltungsstrafgesetzes (VStG).

Das neue Datenschutzregime sieht bei Verstößen gegen die DSGVO Geldbußen in einer Höhe bis zu € 20 Millionen oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs eines Unternehmens, je nachdem, welcher der Beträge höher ist, vor. Dabei ist jedoch zu beachten, dass es sich hierbei um den maximalen Strafrahmen handelt und dieser nur bei systematischen und schwerwiegenden Verstößen Verantwortlicher ausgeschöpft werden kann.

In diesem Zusammenhang führt auch Erwägungsgrund 148 in Bezug auf Art. 83 DSGVO aus, dass im Fall eines geringfügigen Verstoßes oder falls die zu verhängende Geldbuße voraussichtlich eine unverhältnismäßige Belastung für eine natürliche Person darstellen würde, anstelle einer Geldbuße eine Verwarnung erteilt werden kann. Für die genannten Fälle kommt der DSB daher ein „pflichtgemäßes Ermessen“ darüber zu, ob sie bei Verstößen gegen die DSGVO Geldbußen verhängt[4] oder hiervon Abstand nimmt und eine Ermahnung – dann im Sinne des § 45 Abs. 1 letzter Satz VStG – ausspricht. In Anbetracht der Höhe der in Art. 83 leg. cit. angedrohten Geldbußen sowie wegen deren repressiven und abschreckenden Charakters besteht zudem auch kein Zweifel daran, dass es sich bei den Geldbußen gemäß Art. 83 DSGVO um „Strafen“ im Sinne von Art 6 EMRK handelt und daher Beschuldigten im Verfahren vor der Datenschutzbehörde sämtliche Verfahrensgarantien des Art. 6 EMRK zukommen.

ses betreffend Verarbeitungstätigkeiten auferlegt.

4 Vgl. Potacs/Raschauer, Zur Problematik hoher Geldbußen im Unionsrecht - am Beispiel der Datenschutzgrundverordnung, ÖZW 2017, 54.

Das DSG, das in § 62 bestimmte zusätzliche Straftatbestände aufzählt und im Verhältnis zu Art. 83 DSGVO subsidiär zur Anwendung gelangt, sieht Strafen von bis zu € 50.000 vor. In jedem Fall hat sich das Strafmaß für datenschutzrechtliche Verstöße durch die DSGVO im Vergleich zur Rechtslage nach dem DSG 2000, welches Verwaltungsstrafen von höchstens € 25.000 vorsah, erhöht.

Geldbußen gemäß Art. 83 DSGVO können gegen „Verantwortliche“ und „Auftragsverarbeiter“ verhängt werden. Ein „Verantwortlicher“ im Sinne der Begriffsbestimmung in Art. 4 Z 7 DSGVO kann eine „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“ sein. Auftragsverarbeiter ist demgegenüber gemäß Art. 4 Z 8 DSGVO „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Die „Verarbeitung“ umfasst dabei nach Art. 4 Z 4 DSGVO „das Erheben, Erfassen, Speichern, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ von Daten.

Hinsichtlich des Adressatenkreises einer Geldbuße ist hervorzuheben, dass sowohl die DSGVO als auch das DSG die Möglichkeit vorsehen, dass Strafen nicht nur gegen natürliche Personen, sondern auch gegen juristische Personen verhängt werden können. Gegen Behörden, öffentliche Stellen und Körperschaften des öffentlichen Rechts können demgegenüber gemäß § 30 Abs. 5 DSG keine Geldbußen verhängt werden.

Die im Berichtszeitraum höchste, von der Datenschutzbehörde ausgesprochenen Strafe beläuft sich auf € 4.800 (Videoüberwachung eines Geschäftslokals: Filmen des öffentlichen Raums, keine geeigneten Hinweisschilder, zu lange Speicherdauer, keine Protokollierung der Verarbeitungsvorgänge; nicht rechtskräftige Entscheidung DSB-D550.038/0003-DSB/2018). Auch das Filmen des Straßenverkehrs mittels am Armaturenbrett und im Heckbereich eines Kraftfahrzeugs angebrachter Dash-Cams führte zu einer Geldbuße für den Lenker. In einer weiteren – nicht rechtskräftigen Entscheidung – sprach die DSB eine Geldbuße gegen den Mieter einer Wohnung in einem Mehrparteienwohnhaus aus, der mit Hilfe mehrerer Kameras auf unzulässige Weise – unter Anderem auch den vor seiner von ihm bewohnten Wohnung liegenden und zu weiteren Wohnungen anderer Mieter führenden – Gangbereich erfasste und dadurch gegen das Verbot des Filmens von zum höchstpersönlichen Lebensbereich zählenden Bereichen Betroffener verstoßen hat.

Im Kern ist den bislang von der DSB verhängten Straferkenntnissen in Bezug auf den Betrieb privater Videoüberwachungsanalgen gemein, dass diese in Bezug auf deren räumlichen Erfassungsbereich derart betrieben wurden, dass sie Betroffene, wie zufällig in den Erfassungsbereich gelangende Nachbarn oder Straßenverkehrsteilnehmer, in Lebenssituationen erfassten, in welchen die Betroffenen nicht mit einer Bildaufnahme rechnen mussten; sohin lag durch den Betrieb der Bildaufnahme nach Ansicht der DSB ein Verstoß gegen die in Art. 5 DSGVO normierten Grundsätze der Zweckbindung und Datenminimierung vor. Zudem war in den verfahrensgegenständlichen Fällen keine die Rechtmäßigkeit der Datenverarbeitung tragende Rechtsgrundlage iSd Art. 6 Abs. 1 DSGVO ersichtlich. Konkret wurde von der Datenschutzbehörde im Hinblick auf den räumlichen Erfassungsbereich der Videoüberwachungsanlagen (bspw. benachbarte Liegenschaften und öffentliche Verkehrsflächen) auf Seiten der Verantwortlichen kein berechtigtes Interesse am Betrieb der jeweiligen Bildaufnahme erkannt. Vielmehr überwogen in sämtlichen Fällen die (grundrechtlich) geschützten Rechtspositionen auf Geheimhaltung

und Schutz des Privat- und Familienlebens der Betroffenen iSd § 1 DSG bzw. Art. 7 GRC und Art. 8 EMRK ein allfälliges Interesse am Betrieb der gegenständlichen Videoüberwachungsanlagen.

### 3.2.13 Stellungnahmen zu Gesetzes- und Verordnungsvorhaben

Die DSB hat im Jahr 2018 zu folgenden Vorhaben eine Stellungnahme abgegeben. Die Stellungnahmen sind, soweit es sich nicht jene zu Verordnungen oder Landesgesetzen handelt, unter www.parlament.gv.at abrufbar.

Anzumerken ist, dass ein Gutteil der Stellungnahmen Anpassungen in Bundesgesetzen betraf, die als „Materien-Datenschutz-Anpassungsgesetze 2018“ kundgemacht wurden und zu welchen eine Stellungnahme nur innerhalb sehr kurzer Fristen möglich war.

- Datenschutz-Anpassungsgesetz BMI
- PNR-Gesetz
- Wiener Elektrizitätswirtschaftsgesetz 2005 und Wiener Starkstromwegegesetz 1969
- Datenschutzverordnung für die Sozialversicherung
- Datenschutz-Anpassungsgesetz Dienstrecht
- Datenschutz-Anpassungsgesetz BKA
- Datenschutz-Anpassungsgesetz BMLV
- Datenschutz-Anpassungsgesetz Bildung
- Datenschutz-Anpassungsgesetz BMASGK
- Änderung des Weingesetzes
- Änderung des AWG
- Datenschutz-Anpassungsgesetz Wissenschaft und Forschung
- Änderung der BAO und der Abgabenexekutionsordnung
- Datenschutz-Anpassungsgesetz Justiz
- Datenschutz-Anpassungsgesetz BMEIA
- Datenschutz-Anpassungsgesetz BMDW
- Strafprozessrechtsänderungsgesetz 2018 (Ausschussbegutachtung)
- „Sicherheitspaket 2018“ (Ausschussbegutachtung)
- Datenschutz-Anpassungsgesetz BMVIT
- Datenschutz-Anpassungsgesetz Gesundheit
- Datenschutz-Anpassungsgesetz Sozialversicherung
- Verordnung des BMVIT mit der die Führerschein-Alternative Bewährungssystemverordnung, die Gefahrgutbeförderungsverordnung, die Jachtführung-Prüfungsordnung und die Weltraumverordnung geändert werden
- Bundesgesetz, mit dem das Transparenzdatenbankgesetz 2012 geändert wird (Datenschutzanpassung)
- NÖ Datenschutzgesetz 2018
- Bundesgesetz, mit dem das Bundeshaushaltsgesetz 2013 geändert wird
- Datenschutz-Anpassungsgesetz Sport
- Änderung des Bundesgesetzes über die Wahrnehmung konsularischer Aufgaben
- Fremdenrechtsänderungsgesetz 2018
- Verordnung des Bundesministers für Finanzen, mit der die Verordnung über Allgemeine Rahmenrichtlinien für die Gewährung von Förderungen aus Bundesmitteln (ARR 2014) geändert wird
- Entwurf eines Gesetzes, mit dem die Bauordnung für Wien, das Wiener Kleingartengesetz 1996, das Wiener Garagengesetz 2008, das Wasserversorgungsgesetz und das Wiener Wohnbauförderungs- und Wohnhaussanierungsgesetz – WWFSG 1989 geändert werden (Bauordnungsnovelle 2018)
- Entwurf einer Verordnung des Bundesministers für Inneres gemäß § 2 Abs. 5 PNR-G
- Entwurf eines Bundesgesetzes, mit dem das Telekommunikationsgesetz 2003, das

Funkanlagen-Marktüberwachungs-Gesetz und das Funker-Zeugnisgesetz geändert werden soll
- Entwurf eines Gesetzes über die Anpassung der Burgenländischen Landesrechtsordnung an die Datenschutz-Grundverordnung im Agrarwesen
- Verordnung, mit der die Eignungsprüfungsverordnung-Inneres geändert wird
- Entwurf eines Netz- und Informationssystemsicherheitsgesetzes – NISG
- Entwurf eines Bundesgesetzes, mit dem das IKT-Konsolidierungsgesetz, das Signatur- und Vertrauensdienstegesetz, das Unternehmensserviceportalgesetz, das Bundesgesetzblattgesetz, das Zustellgesetz, die Bundesabgabenordnung, das Bundesfinanzgerichtsgesetz, das Meldegesetz 1991, das Passgesetz 1992 und das Personenstandsgesetz 2013 geändert werden
- Stellungnahme der Datenschutzbehörde zum Antrag der Abgeordneten Peter Haubner, Ing. Wolfgang Klinger, Kolleginnen und Kollegen betreffend ein Bundesgesetz, mit dem das Wirtschaftskammergesetz 1998 geändert wird (Ausschussbegutachtung)
- Entwurf eines Bundesgesetzes betreffend Grundsätze für die Sozialhilfe (Sozialhilfe-Grundsatzgesetz) und eines Bundesgesetzes über die bundesweite Gesamtstatistik über Leistungen der Sozialhilfe (Sozialhilfe-Statistikgesetz)
- Novelle des Transparenzdatenbankgesetzes 2012
- Entwurf eines Zivilrechts- und Zivilverfahrensrechts-Änderungsgesetzes 2019
- Entwurf einer Identifikationsverordnung des BMVIT – IVO
- Entwurf der 19. FSG-Novelle

# 4 Wesentliche höchstgerichtliche Entscheidungen

## 4.1 Verfahren vor dem Verfassungsgerichtshof

Im Berichtszeitraum sind keine relevanten datenschutzrechtlichen Entscheidungen des Verfassungsgerichtshofes ergangen.

## 4.2 Oberster Gerichtshof

### 4.2.1 OGH, 6 Ob 23/18b, 28. Februar 2018

Der Oberste Gerichtshof hat in seiner Entscheidung 6 Ob 23/18b vom 28.02.2018[5] (Maximilian Schrems gg. Facebook Ireland) die Revisionsrekurse der klagenden Partei gegen den Beschluss des Oberlandesgerichtes Wien (als Rekursgericht), mit dem der Beschuss des Landesgerichtes für ZRS teilweise abgeändert wurde, als unberechtigt zurückgewiesen.

Der Kläger machte in seiner Klage aus dem Jahr 2014 umfangreiche Feststellungs- und Unterlassungsbegehren u.a. wegen Unwirksamkeit von Vertragsklauseln, der Verwendung der

5 https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20180228_OGH0002_0060OB00023_18B0000_000

Daten zu eigenen Zwecken bzw. Verwendung für Zwecke Dritter sowie Schadenersatz- und Bereicherungsansprüche gegen Facebook im eigenen Namen sowie im Namen von sieben Verbrauchern aus Österreich, Deutschland und Indien geltend. Die internationale Zuständigkeit des Erstgerichts stützte der Kläger primär auf den Verbrauchergerichtsstand (Art. 16 Abs. 1 zweiter Fall EuGVVO alt[6]).

Das Landesgericht für ZRS Wien als Erstgericht wies die Klage zurück, da wegen der auch beruflichen Nutzung von Facebook, der Kläger sich nicht auf den Verbrauchergerichtsstand nach EuGVVO stützen könne und - bezogen auf die Abtretungen - der persönliche Gerichtsstand des Zedenten nicht auf den Zessionar übergehe.

Das Oberlandesgericht Wien als Zweitgericht änderte den Zurückweisungsbeschluss des Erstgerichts dahingehend ab, dass es die Klage nur hinsichtlich der zedierten Ansprüche zurückwies, da die Zuständigkeitsregeln für Verbraucher in der EuGVVO einem Verbraucher nur dann zugute kämen, wenn er persönlich Partei in einem Rechtsstreit sei.

Der vom Kläger erhobene Revisionsrekurs beim OGH wurde – im Wesentlichen gestützt auf die Entscheidung des EuGH im Rahmen eines Vorlageverfahrens zur Auslegung von Art. 15 und Art. 16 Abs. 1 EuGVVO (Verordnung (EG) Nr. 44/2001) – als unberechtigt zurückgewiesen. Der EuGH erkannte, dass ein Nutzer eines privaten Facebook-Kontos die Verbrauchereigenschaft nicht verliert, wenn er Bücher publiziert, Vorträge hält, Websites betreibt, Spenden sammelt und sich die Ansprüche zahlreicher Verbraucher abtreten lässt, um sie gerichtlich geltend zu machen. Gleichzeitig erkannte der EuGH, dass Art 16 Abs. 1 EuGVVO keine Anwendung auf die Klage eines Verbrauchers findet, mit der dieser am Klägergerichtsstand nicht nur seine eigenen Ansprüche geltend macht, sondern auch Ansprüche, die von anderen Verbrauchern mit Wohnsitz im gleichen Mitgliedstaat, in anderen Mitgliedstaaten oder in Drittstaaten abgetreten wurden.

Zusätzlich beschäftigte sich der OGH in seinem Beschluss aber auch mit der Frage, ob aufgrund der - im Jahr 2013 vom selben Kläger direkt beim Irish Data Protection Commissioner - eingebrachten 153-seitigen Beschwerde „vorherige Streitanhängigkeit zum selben „Streitgegenstand“ vorliege und damit das Erstgericht gemäß Art. 27 der Verordnung (EG) Nr 44/2001 sein Verfahren aussetzen kann, bis die Zuständigkeit des zuerst angerufenen Gerichts feststeht. Der OGH erkannte, dass es sich beim Irish Data Protection Commissioner zwar um eine unabhängige, aber dennoch monokratische Verwaltungsbehörde handle, das irische Verfahren in erster Linie öffentlichen Interessen diene, während der Kläger im vorliegenden Verfahren einen zivilrechtlichen Unterlassungstitel begehrt. Das Verfahren vor der irischen Verwaltungsbehörde sei im Kern ein Verwaltungsverfahren, in dem die Behörde den Auftraggeber dazu verpflichtet, bestimmte Gesetzesverstöße abzustellen und einen gesetzmäßigen Zustand herzustellen, daher seien die „Enforcement Notices“ auch nicht als „Entscheidungen“ iSd Art 32 EuGVVO aF bzw Art 2 lit a und Art 36 EuGVVO 2012 anzusehen, zumal darin nicht dem Kläger unmittelbar etwas zugesprochen würde. Zusammenfassend liegt daher bei dem Verfahren vor dem Irish Data Protection Commissioner und dem vorliegenden Verfahren keine Identität des Streitgegenstands vor.

6 Verordnung (EG) Nr. 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (veraltet) https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32001R0044&from=DE

Einer Presseaussendung des Klägers vom 25. Jänner 2019[7] zufolge, hat sich das Landesgericht für Zivilrechtssachen Wien nach Einführung der EU-Datenschutzgrundverordnung (DSGVO) und des neuen Datenschutzgesetzes in Österreich für unzuständig erklärt, da nun nur noch die Datenschutzbehörde, nicht aber „normale" Gerichte für Datenschutzsachen zuständig seien.

### 4.2.2. OGH, 6 Ob 140/18h, 31. August 2018

Der Oberste Gerichtshof hat in seiner Entscheidung 6 Ob 140/18h[8] vom 31.08.2018 eine Revision der beklagten Partei (TV Anbieter) im Rahmen einer Verbandsklage gegen dessen Klauseln in Allgemeinen Geschäftsbedingungen abgewiesen, und festgestellt, dass bei einer Koppelung der Einwilligung zu einer Verarbeitung vertragsunabhängiger personenbezogener Daten mit einem Vertragsabschluss grundsätzlich davon auszugehen ist, dass die Erteilung der Einwilligung nicht freiwillig erfolgt, wenn nicht im Einzelfall besondere Umstände für eine Freiwilligkeit der datenschutzrechtlichen Einwilligung sprechen.

Der OGH hat – wegen der Geltendmachung eines Unterlassungsanspruchs und der dafür erforderlichen Wiederholungsgefahr - in diesem Fall eine Parallelprüfung sowohl nach alter Rechtslage (DSG 2000) als auch nach neuer Rechtslage (DSGVO) vorgenommen. Im Wesentlichen ging es um Klauseln[9] , die den Vertragsabschluss von der Zustimmung zu einer (für die Vertragserfüllung nicht erforderlichen) Datenverwendung (konkret zu Werbezwecken), abhängig machen. In Folge wird nur auf die neue Rechtslage Bezug genommen.

Der OGH schließt aus dem Zusammenwirken von Art. 4 Z 11 DSGVO mit Art. 7 Abs. 4 DSGVO und Erwägungsgrund (43) folgendes: *„Während (...) nach dem Verordnungstext dem Umstand der Koppelung bei der Beurteilung der Freiwilligkeit größtmöglich Rechnung zu tragen ist, spricht der Erwägungsgrund eindeutig für ein unbedingtes Verbot der Koppelung.(...) Das Spannungsverhältnis zwischen dem Text der Verordnung und dem Erwägungsgrund 43 ist offensichtlich dahin aufzulösen, dass an die Beurteilung der „Freiwilligkeit" der Einwilligung strenge Anforderungen zu stellen sind. Bei der Koppelung der Einwilligung zu einer Verarbeitung vertragsunabhängiger personenbezogener Daten mit einem Vertragsschluss ist grundsätzlich davon auszugehen, dass*

---

7 Vgl. https://futurezone.at/netzpolitik/facebook-klage-von-max-schrems-landesgericht-wien-nicht-zustaendig/400388459

8 https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20180831_OGH0002_0060OB00140_18H0000_000

9 Der Kunde stimmt zu, dass die von ihm angegebenen Daten (Name, Geburtsdatum, Adresse, Telefonnummer, EMail-Adresse, Gerätenummer (Client ID) des TVEmpfangsgeräts, Internet ID) von s***** verwendet werden, um dem Kunden Informationen über das Produktportfolio von s*****TV (Aktionen, neue Angebote, neue Programme, Programmhighlights), s***** Internet, TV-Empfangsgeräte, terrestrische Empfangsmöglichkeiten, per Post, E-Mail, Telefon, SMS, Fax oder über soziale Netzwerke zukommen zu lassen sowie zum Datenabgleich gemäß Rundfunkgebührengesetz. Des Weiteren stimmt der Kunde zu, dass die von ihm angegebenen Daten zu den oben angeführten Zwecken an die verbundenen Unternehmen der s***** (O***** GmbH & Co KG, Ö***** GmbH & CO KG, Ö***** Kundenservice GmbH & Co KG, G***** GmbH) übermittelt werden. Diese Zustimmung kann der Kunde jederzeit schriftlich mit Brief oder E-Mail an s***** widerrufen.
Der Kunde stimmt weiters zu, dass die von ihm angegebenen Daten (Name, Geburtsdatum, Adresse, Telefonnummer, E-Mail-Adresse, Gerätenummer (Client ID) des TV-Empfangsgeräts, Internet ID) von s***** verwendet werden, um dem Kunden Informationen über Angebote (Produkte und Leistungen) der Kooperationspartner von s***** per Post, E-Mail, Telefon, SMS, Fax oder über soziale Netzwerke zukommen zu lassen. Kooperationspartner von s***** sind Unternehmen mit Sitz in Österreich, mit welchen s***** bei der Vermarktung der Angebote (Produkte und Leistungen) von s***** zusammenarbeitet und/oder welche ergänzende Leistungen zu den Angeboten von s***** anbietet. Kooperationspartner sind F***** GmbH, O***** GmbH & Co KG, Ö***** GmbH & Co KG, Ö***** Kundenservice GmbH & Co KG und G***** GmbH.Firmenbuchnummer *****. Diese Zustimmung kann der Kunde jederzeit schriftlich mit Brief oder E-Mail an s***** widerrufen."

*die Erteilung der Einwilligung nicht freiwillig erfolgt, wenn nicht im Einzelfall besondere Umstände für eine Freiwilligkeit der datenschutzrechtlichen Einwilligung sprechen (…)“*

## 4.3 Verwaltungsgerichtshof

### 4.3.1 VwGH, Ro 2016/04/0051, 23. Oktober 2017

Ein Beschwerdeführer brachte Beschwerde bei der Datenschutzkommission (nunmehr: Datenschutzbehörde) ein und begründete dies damit, in seinem Recht auf Geheimhaltung verletzt worden zu sein, in dem der Beschwerdegegner (das Finanzamt XY) über Anfrage eines Journalisten Auskunft über ein anhängiges Verfahren wegen des Verdachts von - vom Beschwerdeführer begangene - Verwaltungsübertretungen gegeben habe.

Die Datenschutzbehörde gab der Beschwerde statt und stellte fest, dass der Beschwerdegegner den Beschwerdeführer in seinem Recht auf Geheimhaltung verletzt hat. Das Bundesverwaltungsgericht (BVwG) bestätigte den Bescheid der Datenschutzbehörde.

Die vom Beschwerdegegner (nunmehr: Revisionswerber) erhobene Revision wies der VwGH ab. Er begründete dies im Wesentlichen damit, dass das Recht auf Geheimhaltung gemäß § 1 Abs. 1 DSG 2000 nicht auf automationsunterstützt verarbeitete Daten oder manuelle Daten eingeschränkt ist, sondern auch die mündliche Bekanntgabe bzw. Bestätigung, dass gegen eine bestimmte Person Ermittlungen geführt werden, das Recht auf Geheimhaltung gemäß § 1 Abs. 1 DSG 2000 verletzt.

Der VwGH sprach weiter aus, dass die generalklauselartige Ermächtigung in § 8 Abs. 4 Z 3 DSG 2000 keinen Rechtfertigungstatbestand für die Verwendung strafrechtsbezogener Daten durch Auftraggeber des öffentlichen Bereichs (hier: durch den Beschwerdegegner) bildet. Eine gesonderte einschlägige (materien)gesetzliche Regelung, die eine solche Auskunftserteilung tragen könnte, war im vorliegenden Fall nicht ersichtlich, weshalb das BVwG die Anwendbarkeit des § 8 Abs. 4 Z 3 DSG 2000 zu Recht verneint hat.

### 4.3.2 VwGH, Ra 2017/04/0032, 26. Juni 2018

Zur Vorgeschichte dieses Falls: Die Beschwerdeführerin brachte zunächst eine Beschwerde an das Hochkommissariat für Menschenrechte der Vereinten Nationen (im Folgenden: Hochkommissariat) gemäß dem Fakultativprotokoll zur Konvention zur Beseitigung jeder Form von Diskriminierung der Frau (im Folgenden: Fakultativprotokoll) ein. In dieser Beschwerde wurde unter anderem auf ein vom Landeskriminalamt Niederösterreich (LKA NÖ) erstelltes Protokoll Bezug genommen, das im Zuge von Ermittlungen gegen die Beschwerdeführerin wegen des Verdachts der illegalen Prostitution aufgenommen worden war. Dieses Protokoll enthält (sensible) Daten über das Sexualleben der Beschwerdeführerin, wobei diese ausführt, sie sei im Zuge der Erstellung der Niederschrift sexuell gedemütigt worden.

Aus dem Fakultativprotokoll ergibt sich die Pflicht der Republik Österreich, Darlegungen zur Klärung der Sache zu übermitteln und somit am Verfahren zur Prüfung der Beschwerde bzw. der vorgebrachten Rechtsverletzung vor dem Hochkommissariat mitzuwirken.

Zum datenschutzrechtlichen Fall selbst: Die Beschwerdeführerin erhob bei der Datenschutzbehörde Beschwerde wegen Verletzung im Recht auf Geheimhaltung ihrer personenbezogenen Daten. Sie behauptete, das Bundeskanzleramt (BKA) und das Bundesministerium für Europa,

Integration und Äußeres (BMEIA) hätten als Prozessvertreter Österreichs im Beschwerdeverfahren vor dem Hochkommissariat die Niederschrift des LKA NÖ, die sensible Daten der Beschwerdeführerin enthalte, ohne Einverständnis der Beschwerdeführerin verbreitet.

Die Datenschutzbehörde wies die datenschutzrechtlichen Beschwerden der Beschwerdeführerin ab. Gegen den Bescheid der Datenschutzbehörde beschwerte sich die Frau beim Bundesverwaltungsgericht. Auch das Bundesverwaltungsgericht wies die Beschwerde ab. Gegen das Erkenntnis des Bundesverwaltungsgerichts erhob die Frau Revision an den VwGH.

Der VwGH wies die Revision der Frau ebenfalls ab. Dies begründete der VwGH im Wesentlichen damit, dass die behaupteten Rechtsverstöße im Zusammenhang mit der Erstellung der Niederschrift durch LKA NÖ nicht den Beschwerdegegnern BKA und BMEIA zurechenbar waren.

### 4.3.3. VwGH, Ra 2017/04/0080, 16. Mai 2018

Die Bezirkshauptmannschaft Feldkirch bestrafte einen Mann wegen des nicht gemeldeten Betriebs einer Videoüberwachung gemäß § 52 Abs. 2 Z 1, 6 und 7 DSG 2000 mit einer Geldstrafe in Höhe von EUR 650,-. Gleichzeitig verhängte die Bezirkshauptmannschaft Feldkirch noch eine weitere Strafe und zwar erklärte sie eine Micro SD Speicherkarte des Mannes für verfallen.

Gegen das Straferkenntnis der Bezirkshauptmannschaft Feldkirch erhob der Mann Beschwerde an das Landesverwaltungsgericht Vorarlberg (LVwG Vorarlberg). Dieses wies seine Beschwerde ab. In Folge erhob der Mann Revision an den VwGH. Der VwGH hob das Erkenntnis des LVwG Vorarlberg hinsichtlich des ausgesprochenen Verfalls der Micro SD Speicherkarte auf und begründete seine Entscheidung damit, dass das LVwG Vorarlberg nicht ausreichend begründet hat, warum es die Strafe des Verfalls der Micro SD Speicherkarte für notwendig bzw. verhältnismäßig hielt.

## 4.4 Europäischer Gerichtshof für Menschenrechte

### 4.4.1 EGMR, Ben Faiza v. France, 08.02.2018 – 31446/12

Dieser Fall betraf Überwachungsmaßnahmen, die gegen den Kläger im Rahmen einer Strafuntersuchung, aufgrund seiner Beteiligung an Drogenhandelsdelikten, ergriffen worden waren. Konkret handelte es sich bei den Maßnahmen um die Installation einer Geolokalisierungsvorrichtung an seinem Fahrzeug als auch um einen Gerichtsbeschluss gegenüber einem Mobilfunkbetreiber, welcher Aufzeichnungen über seine eingehenden und ausgehenden Anrufe sowie die Pings des Mobilfunkmastes von seinen Telefonen aus erhält und so eine spätere Verfolgung der Bewegungen des Klägers ermöglicht. Der Kläger machte geltend, dass diese Maßnahmen einen Eingriff in sein Recht auf Achtung seines Privatlebens darstellen.

Der EGMR hielt fest, dass am 3. Juni 2010 ein Verstoß gegen Art. 8 EMRK hinsichtlich der Echtzeit-Geolokalisierung des Fahrzeuges des Klägers mittels eines GPS-Gerätes erfolgte. Zudem gab das französische Recht zum relevanten Zeitpunkt im Bereich der Echtzeit-Geolokalisierungsmaßnahmen nicht hinreichend klar an, in welchem Umfang und auf welche Weise die Behörden berechtigt waren, von ihrem Ermessensspielraum Gebrauch zu machen. Der Kläger hatte daher nicht den Mindestschutz durch den Rechtsstaat in einer demokratischen Gesellschaft genossen. Der EGMR stellte jedoch auch fest, dass Frankreich in der Folgezeit einen legislativen Mechanismus zur Regelung der Nutzung von Geolokalisierung und zur Stärkung des Rechts auf Achtung der Privatsphäre angenommen hatte (Gesetz vom 28. März 2014). Ferner

hielt der EGMR fest, dass kein Verstoß gegen Art. 8 EMRK im Zusammenhang mit dem am 24. Juli 2009 an einen Mobilfunkbetreiber ergangenen Gerichtsbeschluss vorliegt, die Liste der vom Telefon des Klägers festgelegten Mobilfunkmasten zur späteren Verfolgung seiner Bewegungen zu erhalten. Der EGMR stellte insbesondere fest, dass die gerichtliche Entscheidung eine Beeinträchtigung des Privatlebens des Klägers darstellt, aber mit dem Gesetz vereinbar ist. Darüber hinaus zielte die Anordnung darauf ab, die Wahrheit im Rahmen von Strafverfahren wegen der Einfuhr von Drogen in eine kriminelle Organisation und Geldwäsche festzustellen, und verfolgte damit die legitimen Ziele der Prävention von Störungen, Verbrechen und des Schutzes der öffentlichen Gesundheit. Der EGMR vertrat auch die Auffassung, dass die Maßnahme in einer demokratischen Gesellschaft notwendig war, weil sie darauf abzielte, eine große Operation des Drogenhandels zu unterbinden. Schließlich waren die erhaltenen Informationen in einer Untersuchung und einem Strafverfahren verwendet worden, in welchem dem Kläger eine wirksame und rechtsstaatliche Überprüfung garantiert worden war.

### 4.4.2 EGMR, Libert v. France, 22.02.2018 – 588/13

In diesem Fall ging es um die Entlassung eines Mitarbeiters der SNCF (Französische Staatsbahn), nachdem die Beschlagnahmung seines Arbeitscomputers die Speicherung von pornographischen Dateien und gefälschten Zertifikaten für Dritte ergeben hatte. Der Kläger beschwerte sich insbesondere darüber, dass sein Arbeitgeber in seiner Abwesenheit persönliche Dateien eingesehen habe, die auf der Festplatte seines Arbeitsrechners gespeichert waren.

Der EGMR stellte fest, dass kein Verstoß gegen Art. 8 EMRK vorliegt und die französischen Behörden im vorliegenden Fall den ihnen zur Verfügung stehenden Ermessensspielraum nicht überschritten hatten. Der EGMR hielt insbesondere fest, dass die Einsichtnahme des Arbeitgebers in die Dateien ein legitimes Ziel verfolgt hatte, da der Arbeitgeber zu Recht sicherstellen wollte, dass seine Arbeitnehmer die ihnen zur Verfügung gestellten Computer im Einklang mit ihren vertraglichen Verpflichtungen und den geltenden Vorschriften nutzen. Der EGMR stellte ferner fest, dass das französische Recht einen Mechanismus zum Schutz der Privatsphäre umfasst, der es Arbeitgebern ermöglicht, berufliche Dateien einzusehen, wobei Arbeitgeber nicht heimlich Dateien einsehen können, die als personenbezogen identifiziert wurden. Die letztgenannten Dateien können nur in Anwesenheit des betroffenen Mitarbeiters eingesehen werden. Die inländischen Gerichte hatten entschieden, dass der genannte Mechanismus den Arbeitgeber nicht daran gehindert hätte, die fraglichen Dateien zu öffnen, da sie nicht als privat gekennzeichnet waren. Schließlich vertrat der EGMR die Auffassung, dass die inländischen Gerichte die Behauptung des Klägers über eine Verletzung seines Rechts auf Achtung seines Privatlebens ordnungsgemäß geprüft hatten und, dass die Entscheidungen dieser Gerichte auf triftigen und ausreichenden Gründen beruhten.

### 4.4.3 EGMR, Benedik v. Slovenia, 24.04.2018 – 62357/14

Dieser Fall betraf die Tatsache, dass die slowenische Polizei keinen Gerichtsbeschluss über den Zugang zu Teilnehmerinformationen im Zusammenhang mit einer dynamischen IP-Adresse hatte, welche von den Schweizer Strafverfolgungsbehörden während der Überwachung der Nutzer eines bestimmten Filesharing-Netzwerks erfasst wurden. Der Zugriff auf diese Teilnehmerinformationen führte dazu, dass der Kläger identifiziert wurde, nachdem er Dateien über das Netzwerk geteilt hatte, einschließlich Kinderpornographie.

Der EGMR hielt fest, dass ein Verstoß gegen Art. 8 EMRK vorliegt, da die von der Polizei, zur Erlangung der mit der dynamischen IP-Adresse verbundenen Teilnehmerinformationen, verwendete Rechtsvorschrift nicht dem Übereinkommensstandard „in Übereinstimmung mit dem Gesetz“ entsprach. Die Bestimmung war unklar, bot praktisch keinen Schutz vor willkürlichen

Eingriffen, hatte keine Schutzmaßnahmen gegen Missbrauch und keine unabhängige Überwachung der beteiligten Polizeikräfte.

### 4.4.4 EGMR, Centrum För Rättvisa v. Sweden, 19.06.2018 – 35252/08

Dieser Fall betraf eine Beschwerde einer Anwaltskanzlei, welche Personen bei der Rechtsdurchsetzung gegenüber dem Staat vertritt, in der behauptet wurde, dass die Gesetzgebung, welche das Abfangen elektronischer Signale in Schweden für ausländische Nachrichtendienste erlaubt, gegen die geltenden Datenschutzbestimmungen verstößt.

Der EGMR hielt fest, dass in der vorliegenden Rechtssache kein Verstoß gegen Art. 8 EMRK vorlag. Die Anwaltskanzlei vertrat insbesondere die Auffassung, dass die einschlägigen Rechtsvorschriften ein System der geheimen Überwachung darstellen, das potenziell alle Nutzer von Mobiltelefonen und Internet betrifft, ohne, dass sie über die Überwachung benachrichtigt werden. Außerdem gäbe es keinen nationalen Rechtsbehelf, welcher einer betroffenen Person, die vermute, dass ihre Mitteilungen abgefangen worden seien, die Möglichkeit der Erhebung eines Rechtsmittels dagegen bot. Auf dieser Grundlage hielt der EGMR es für gerechtfertigt, die nationalen Rechtsvorschriften in ihrer Gesamtheit zu prüfen. Im Zuge dessen stellte der EGMR fest, dass das schwedische System des Massenabfangens insgesamt ausreichende Garantien gegen Willkür und die Gefahr vor Missbrauch bietet, auch wenn es einige verbesserungsfähige Bereiche gibt. Insbesondere der Umfang der Maßnahmen zur Signalaufklärung und die Behandlung der abgefangenen Daten waren rechtlich klar definiert. Zudem musste die Bewilligung zum Abfangen nach einer eingehenden Prüfung gerichtlich erteilt werden und bezog sich nur auf Mitteilungen, welche über die schwedische Grenze hinaus ergingen und nicht innerhalb Schwedens selbst erfolgten. Die gerichtliche Bewilligung durfte weiters nur für maximal sechs Monate erteilt werden und erforderte jede Verlängerung eine neuerliche Überprüfung. Darüber hinaus gab es mehrere unabhängige Stellen, insbesondere eine Aufsichtsbehörde, die mit der Überwachung und Überprüfung des Systems beauftragt war. Schließlich wurde die fehlende Meldung von Überwachungsmaßnahmen gegenüber betroffenen Personen dadurch kompensiert, dass eine Reihe von Beschwerdemechanismen zur Verfügung standen, insbesondere durch die Aufsichtsbehörde, die Parlamentarischen Bürgerbeauftragten und den Justizkanzler. Bei seiner Schlussfolgerung berücksichtigte der EGMR den Ermessensspielraum des Staates beim Schutz der nationalen Sicherheit, insbesondere angesichts der derzeitigen Bedrohungen durch den globalen Terrorismus und die schwere grenzüberschreitende Kriminalität.

### 4.4.5 EGMR, Big Brother Watch and Others v. the United Kingdom, 13.09.2018 – 58170/13, 62322/14 und 24960/15

Diese Anträge wurden eingereicht, nachdem Edward Snowden (ehemaliger Auftragnehmer der US National Security Agency) Informationen über Programme zur Überwachung und zum Austausch von Daten zwischen den USA und dem Vereinigten Königreich preisgegeben hatte. Der Fall betraf Beschwerden von Journalisten und Bürgerrechtsorganisationen über drei Arten der Überwachung: die weitgehende Überwachung von Kommunikationen, den Austausch von Informationen mit ausländischen Regierungen und die Beschaffung von Kommunikationsdaten von Dienstanbietern.

Der EGMR stellte fest, dass die Massenabhörregelung gegen Art. 8 EMRK verstößt, da sowohl die Auswahl der Internetinhaber zum Abfangen als auch die Filterung, Suche und Auswahl der abgefangenen Mitteilungen zur Prüfung unzureichend überwacht wurden und die Garantien für die Auswahl der „verwandten Kommunikationsdaten“ zur Prüfung unzureichend waren. In seiner Schlussfolgerung hielt der EGMR fest, dass eine Massenabhörregelung an sich nicht gegen das Übereinkommen verstößt, stellte aber fest, dass eine solche Regelung die in seiner

Rechtsprechung festgelegten Kriterien erfüllen muss. Der Gerichtshof hielt ebenfalls fest, dass die Regelung zur Beschaffung von Kommunikationsdaten von Kommunikationsdiensteanbietern gegen Art. 8 EMRK verstößt, da sie nicht im Einklang mit dem Gesetz steht und dass sowohl die Regelung zur Massenabhörung als auch die Regelung zur Beschaffung von Kommunikationsdaten von Kommunikationsdiensteanbietern gegen Art. 10 EMRK verstoßen, da es keine ausreichenden Garantien in Bezug auf vertrauliches journalistisches Material gibt. Der EGMR stellte ferner fest, dass das System für den Austausch von Informationen mit ausländischen Regierungen weder gegen Art. 8 noch gegen Art. 10 EMRK verstößt. Schließlich wies der EGMR Beschwerden der dritten Gruppe von Antragstellern wegen Art. 6 EMRK, über das innerstaatliche Verfahren zur Anfechtung geheimer Überwachungsmaßnahmen, und wegen Art. 14 EMRK zurück.

## 4.5 Europäischer Gerichtshof

### 4.5.1 C-210/16 (Wirtschaftsakademie Schleswig-Holstein), Urteil vom 5. Juni 2018

Der EuGH hat am 5. Juni 2018 im Rahmen eines Vorabentscheidungsverfahrens (ULD Schleswig-Holstein vs. Facebook Ireland Ltd.) eine richtungsweisende Entscheidung –basierend auf der RL 95/46/EG - getroffen. Demnach ist Art. 2 lit. d der RL 95/46/EG dahingehend auszulegen, dass der Begriff des „für die Verarbeitung Verantwortlichen“ im Sinne dieser Bestimmung den Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fan-Page umfasst.

Die entscheidungsgegenständliche Verarbeitung erfolgt so, dass Facebook auf dem Computer oder einem anderen Endgerät, mit dem die Fan-Page besucht wird, Cookies platziert. Facebook verarbeitet in Folge die - in den Cookies gespeicherten - Informationen, insbesondere um sein System der Werbung zu verbessern, aber auch um den Betreibern der Fan-Page Statistiken zur Verfügung zu stellen, um deren Vermarktung zu verbessern. Der Betreiber einer Facebook Fan-Page muss bei der Einrichtung seiner Fan-Page eine Parametrierung u. a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten vornehmen. Damit ist er an der Entscheidung über Zwecke und Mittel der Verarbeitung personenbezogener Daten der Fan-Page Besucher beteiligt. Erfasst und verarbeitet werden nicht nur Daten von Besuchern, die selbst ein Facebook-Konto haben, sondern auch von jenen, die über kein Facebook-Konto verfügen. Folgerichtig stuft daher der EuGH den Betreiber der Fan-Page im vorliegenden Fall als in der Union gemeinsam mit Facebook Ireland für diese Verarbeitung Verantwortlichen im Sinne von Art. 2 lit d der RL 95/46/EG ein.

Abschließend sei angemerkt, dass sich die Definition des datenschutzrechtlich Verantwortlichen in Art. 2 lit der RL 95/46/EG nicht von jener in Art. 4 Abs. 7 der DSGVO unterscheidet. Zudem sieht Art. 26 DSGVO spezielle Regelungen von „Gemeinsam Verantwortlichen“ vor, sodass die Relevanz der EuGH Entscheidung auch unter dem DSGVO Regime gegeben ist.

### 4.5.2 C-25/17 (Zeugen Jehovas), Urteil vom 10. Juli 2018

In diesem Vorabentscheidungsverfahren hatte der EuGH zu beurteilen, ob die Verkündungstätigkeit von „Tür zu Tür“ einer Religionsgemeinschaft unter die RL 95/46/EG fällt oder als „Tätigkeit für ausschließlich persönliche oder familiäre“ Zwecke zu werten ist und somit nicht unter die RL 95/46/EG fällt.

Der EuGH hat diese Frage dahingehend beantwortet, dass eine solche Tätigkeit unter die RL 95/46/EG fällt und diese daher zu beachten ist.

Weiters war die Frage zu klären, ob die handschriftlichen Aufzeichnungen, die von den verkündenden Mitgliedern im Zuge der Verkündungstätigkeit von Tür zu Tür gemacht werden, eine „Datei" im Sinne von Art. 2 lit c RL 95/46/EG sind. Der EuGH geht hier von einem weiten Dateibegriff aus und verlangt nur, dass die Daten nach bestimmten Kriterien, die eine leichte Wiederauffindbarkeit der personenbezogenen Daten einer Person gewährleisten, strukturiert sein müssen. Um unter diesen Begriff zu fallen, muss eine solche Datensammlung nicht aus spezifischen Kartotheken oder Verzeichnissen oder anderen der Recherche dienenden Ordnungssystemen bestehen.

Zuletzt war strittig, wer im Falle einer Verkündungstätigkeit von „Tür zu Tür" als Verantwortlicher der Datenverarbeitung anzusehen ist – das verkündende Mitglied oder die dahinterstehende Religionsgemeinschaft. Der EuGH hat ausgesprochen, dass aufgrund der Umstände des Ausgangsverfahrens eine gemeinsame Datenverarbeitung vorliegt und dass verkündende Mitglieder und die Religionsgemeinschaft als gemeinsam Verantwortliche zu werten sind. Dafür ist es nicht erforderlich, dass die Religionsgemeinschaft Zugriff auf diese Daten hat oder ihren Mitgliedern nachweislich schriftliche Anleitungen oder Anweisungen zu diesen Datenverarbeitungen gegeben hat. Die Verkündungstätigkeit von „Tür zu Tür" dient nämlich der Verbreitung des Glaubens der Religionsgemeinschaft. Darüber hinaus stellt diese Verkündungstätigkeit eine wesentliche Betätigungsform der Gemeinschaft dar.

Das Urteil erging zur RL 95/46/EG, ist jedoch für die DSGVO von Relevanz, weil die wesentlichen Definitionen in der RL 95/46/EG und in der DSGVO nicht voneinander abweichen (vgl. zum Begriff des „Dateisystems" nunmehr Art. 4 Z 6 DSGVO).

### 4.5.3 C-40/17 (Fashion ID), Schlussanträge des Generalanwalts vom 19. Dezember 2018

Der Generalanwalt legte im Rahmen des Verfahrens zum Vorabentscheidungsersuchen des Oberlandesgericht Düsseldorf seine Schlussanträge vor. Im gegenständlichen Verfahren reichte die Verbraucherzentrale NRW e. V. (ein deutscher Verbraucherschutzverband) eine Unterlassungsklage gegen die Fashion ID GmbH & Co. KG ein. Die Fashion ID ist ein Onlinehändler für Mode-Artikel. In ihrer Webseite ist ein Plugin, der Facebook „Gefällt mir"-Button, eingebunden. Besucht ein Nutzer diese Webseite, so werden Facebook Informationen über die IP-Adresse dieses Nutzers und der Browser-String übermittelt. Unabhängig davon, ob der Nutzer den „Gefällt mir"-Button tatsächlich angeklickt hat oder über ein Facebook-Konto verfügt, erfolgt die Übermittlung automatisch beim Laden der gegenständlichen Website. Darüber hinaus platziert Facebook unterschiedliche Cookies auf dem Gerät des Nutzers. Ziel der Unterlassungsklage ist es daher, der Fashion ID die Verwendung des „Gefällt-mir"-Buttons zu untersagen. Die zentrale Frage des gegenständlichen Vorabentscheidungsersuchens ist jene der datenschutzrechtlichen Rollenverteilung zwischen Fashion ID und Facebook.

Zunächst hielt der Generalanwalt fest, dass die RL 95/46/EG einem nationalen Verbandsklagerecht für Verbraucherschutzverbände nicht entgegensteht und verweist auf die DSGVO, die den Mitgliedstaaten gemäß Art. 80 Abs. 2 DSGVO nunmehr die Möglichkeit einräumt, entsprechende innerstaatliche Regelungen zu treffen, sodass u.a. ein Verbraucherschutzverband - unabhängig von einem Auftrag der betroffenen Person - eine Beschwerde bei der zuständigen Aufsichtsbehörde einlegen kann.

In weiterer Folge nimmt der Generalanwalt auf die Entscheidung der Rechtssache C-210/16 (Wirtschaftsakademie Schleswig-Holstein) Bezug und führt aus, dass die dort genannte Pa-

rametrierung ein entscheidender Faktor für die Beteiligung an Zwecke und Mittel der Verarbeitung personenbezogener Daten ist. Auch nimmt er auf die Entscheidung in der Rechtssache C-25/17 (Zeugen Jehovas) Bezug und führt aus, dass der gemeinsam Verantwortliche nicht notwendigerweise auch Zugriff auf die personenbezogenen Daten haben muss.

Im gegenständlichen Fall platziert Fashion ID das Plugin auf ihrer Website, wodurch es Facebook erst ermöglicht wird, personenbezogene Daten der Nutzer zu erhalten. Im Unterschied zu den vorangegangenen Fällen vor dem EuGH führt die Fashion ID keine Parametrierung durch, allerdings liegt der angestrebte Nutzen in der kostenlosen Werbung für ihre Produkte.

Der Generalanwalt kommt zu dem Ergebnis, dass Fashion ID durch Einbindung eines Plugins eines Dritten die Erhebung und Übermittlung personenbezogener Daten eines Nutzers veranlasst (wobei der Dritte, also Facebook, das Plugin bereitgestellt hat) und Fashion ID daher als ein für die Verarbeitung Verantwortlicher anzusehen ist. Die gemeinsame Verantwortlichkeit ist nach Ansicht des Generalanwalts allerdings auf Verarbeitungsvorgänge beschränkt, für die Fashion ID tatsächlich einen Beitrag zur Entscheidung über die Mittel und Zwecke der Verarbeitung personenbezogener Daten leistet.

Die Einwilligung und die Informationspflichten müssen überdies vor der entsprechenden Erhebung und Übermittlung eingeholt bzw. umgesetzt werden. Der Generalanwalt berücksichtigt dabei den Hinweis der Kommission, wonach Webseiten-Besucher, die über ein Facebook-Nutzerkonto verfügen, gegebenenfalls bereits zu einem früheren Zeitpunkt in eine solche Datenübermittlung eingewilligt haben könnten. Diese Auffassung teilt er jedoch nicht, da durch diese Argumentation impliziert wird, dass man mit Erstellung eines Facebook-Nutzerkontos im Voraus in jegliche Datenverarbeitung einwilligt, die im Zusammenhang mit Online-Aktivitäten solcher „Facebook-Nutzer“ durch Dritte erfolgt.

Es bleibt abzuwarten, ob der EuGH den Schlussanträgen des Generalanwalts folgt und falls ja, in welcher Detailgenauigkeit er diese übernimmt. Angesichts der praktischen Relevanz der datenschutzrechtlichen Rollenverteilung im Zusammenhang mit (Werbe-) Cookies wird das Urteil des EuGH jedenfalls richtungsweisend sein.

# 5 Datenschutz-Grundverordnung: Erste Erfahrungen der Datenschutzbehörde und legistische Maßnahmen

Ebenso wie in den Jahren 2016 und 2017 war das 1. Halbjahr 2018 den intensiven Vorbereitungen auf das Ingeltungtreten der Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 gewidmet. Darüber hinaus waren konkrete Umsetzungsmaßnahmen zu treffen, um einen reibungslosen Übergang von der Rechtslage nach dem DSG 2000 zur Rechtslage nach der DSGVO und dem DSG zu gewährleisten. Der seit 25. Mai 2018 verstrichene Zeitraum gestattete es darüber hinaus, erste Erfahrungen zu sammeln.

## 5.1. Vorbereitungsmaßnahmen:

### 5.1.1 Aufnahme und Einschulung zusätzlicher Bediensteter

Im Berichtszeitraum lag der Fokus u.a. auf der Aufnahme und Einschulung zusätzlicher Bediensteter. Der Datenschutzbehörde wurden in den Bundesfinanzgesetzen 2018 und 2019 fünf zusätzliche Planstellen des höheren Dienstes sowie eine Sonderplanstelle des höheren Dienstes und weiters zwei Stellen für Verwaltungspraktikanten bewilligt.

Die neuen Bediensteten, die aus anderen Bereichen der Bundesverwaltung kamen, konnten rasch in den bestehenden Mitarbeiterstab integriert und eingeschult werden.

### 5.1.2. Neue Struktur der Datenschutzbehörde und interne Maßnahmen

Durch den zu erwartenden zusätzlichen Arbeitsanfall, verbunden mit neuen Aufgaben, die nach der DSGVO der Datenschutzbehörde übertragen wurden, war eine Umstrukturierung der Behörde erforderlich. Die Datenschutzbehörde wurde in insgesamt 6 Büros unterteilt, die die verschiedenen Aufgaben wahrnehmen.

Es sind dies:

- Büro 1: Präsidium
- Büro 2: Verfahrensführung
- Büro 3: Internationales und grenzüberschreitende Zusammenarbeit
- Büro 4: Akkreditierungen und Verhaltensregeln
- Büro 5: Verwaltungsstrafen
- Büro 6: Stammzahlenregister (aufgelöst mit Ablauf des 27. Dezember 2018 infolge Übergang der Zuständigkeit auf die Bundesministerin für Digitalisierung und Wirtschaftsstandort)

Die meisten Bediensteten sind zwei Büros zugeteilt. Dies deswegen, um eine zu starke Spezialisierung und „Verengung“ hintanzuhalten. Bei Bediensteten des Büros 5 ist sichergestellt, dass diese nicht auch den Büros 2 bis 4 zugeteilt sind, um eine unvoreingenommene Verfahrensführung zu gewährleisten.

Alle Verfahren (Beschwerdeverfahren, amtswegige Prüfverfahren, Meldungen über Sicherheitsverletzungen), die bei der Datenschutzbehörde von Personen in Österreich anhängig gemacht werden, werden vom Büro 2 geführt. Stellt sich heraus, dass eine Partnerbehörde in einem anderen Mitgliedstaat zu involvieren ist (Art. 60 ff DSGVO), wird diese kontaktiert.

Verfahren, die bei einer Partnerbehörde in einem anderen Mitgliedstaat anhängig gemacht werden und in welche die Datenschutzbehörde einzubeziehen ist (Art. 60 ff DSGVO) sowie Angelegenheiten des internationalen Datenverkehrs (Kapitel V DSGVO) und die Vertretung der Datenschutzbehörde in den Untergruppen des Europäischen Datenschutzausschusses (EDSA), obliegen dem Büro 3. Das Büro 3 unterstützt auch die Leiterin der Datenschutzbehörde in ihrer Funktion als Vorsitzende des EDSA.

Anträge auf Genehmigung von Verhaltensregeln sowie die Akkreditierung von Überwachungs- und Zertifizierungsstellen fallen in die Zuständigkeit des Büros 4.

Verwaltungsstrafverfahren nach Art. 83 DSGVO und § 62 DSG werden vom Büro 5 geführt.

Das Büro 6 hatte bis zu seiner Auflösung Angelegenheiten des Stammzahlenregisters nach dem E-Governmentgesetz zu betreuen.

Bis zum 25. Mai 2018 waren auch alle von der Datenschutzbehörde verwendeten Formulare sowie die Website an die DSGVO und das DSG anzupassen sowie neue Formulare (v.a. für Verwaltungsstrafen) zu erstellen.

### 5.1.3. Verordnungen der Datenschutzbehörde

Als weitere Vorbereitungsmaßnahme, die vor dem 25. Mai 2018 getroffen wurde, ist die Verordnung über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) anzuführen. Diese wurde am 25. Mai 2018 im BGBl. II Nr. 108/2018 kundgemacht.

### 5.1.4. Information von Behörden

Es wurden alle wesentlichen Bundes-, Landes- und Gemeindebehörden über die Pflicht zur Bestellung eines Datenschutzbeauftragten und zur Meldung des Datenschutzbeauftragten an die Datenschutzbehörde informiert.

Weiters wurden alle Bezirksverwaltungsbehörden in Kenntnis gesetzt, dass die zum Stichtag 24. Mai 2018 bei ihnen anhängigen Verwaltungsstrafverfahren nach § 52 DSG 2000 zuständigkeitshalber an die Datenschutzbehörde abzutreten sind.

### 5.1.5. Legistische Änderungen

Die zweimalige Novellierung des DSG mit BGBl. I Nr. 23/2018 und 24/2018 fiel zwar nicht in den Zuständigkeitsbereich der Datenschutzbehörde, hatte aber Auswirkungen auf sie.

Zunächst wurde § 11 DSG novelliert und die „Verwarnung durch die Datenschutzbehörde“ eingeführt.

Weiters wurde § 35 Abs. 2 DSG geändert und klargestellt, dass die Datenschutzbehörde ihre Befugnisse nicht nur gegenüber den obersten Organen der Vollziehung ausübt, sondern auch gegenüber den Präsidenten des Nationalrates, des Rechnungshofes und des Verwaltungsgerichtshofes sowie gegenüber dem Vorsitzenden der Volksanwaltschaft „im Bereich der diesen zustehenden Verwaltungsangelegenheiten“.

Die Novellierung des Grundrechts auf Datenschutz nach § 1 DSG (Einschränkung auf natürliche Personen) kam mangels Vorliegen des erforderlichen Quorums nicht zustande.

## 5.2. Umsetzungsmaßnahmen

Der 25. Mai 2018 bedingte folgende Änderungen:

- Übernahme anhängiger Verwaltungsstrafverfahren von den Bezirksverwaltungsbehörden (in Summe: 75) und Fortführung bzw. Einstellung dieser Verfahren unter Beachtung des Günstigkeitsprinzips (§ 69 Abs. 5 DSG)
- Fortführung anhängiger Verfahren nach den Bestimmungen der DSGVO bzw. des DSG sowie Einstellung anhängiger Verfahren, wenn deren Fortführung nach der DSGVO nicht mehr erforderlich war (betraf v.a. Verfahren nach § 13 DSG 2000)
- Einstellung des Datenverarbeitungsregisters (DVR) und Bewahrung desselben als Archiv bis

Ende 2019
- Einstellung aller anhängigen Registrierungsverfahren nach §§ 17 ff DSG 2000
- Einnahme der neuen Bürostruktur
- Einbindung von Partnerbehörden in grenzüberschreitenden Fällen

Durch die mehrjährige intensive Vorbereitung ist der Übergang auf die neue Rechtslage ohne nennenswerte Probleme möglich gewesen. Die ersten Bescheide nach der neuen Rechtslage wurden bereits am 28. Mai 2018 erlassen.

Im Berichtszeitraum wurde – nach Durchführung eines innerstaatlichen Begutachtungsverfahrens und des Kohärenzverfahrens im EDSA nach Art. 64 ff DSGVO – die Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) im BGBl. II Nr. 278/2018 kundgemacht.

## 5.3. Erste Erfahrungen der Datenschutzbehörde

### 5.3.1. Anstieg der Verfahrenszahlen

Die Anzahl der bei der Datenschutzbehörde anhängig gemachten Verfahren ist im Vergleich zum Berichtsjahr 2017 signifikant angestiegen.

Die Beschwerdeverfahren betreffen im Wesentlichen alle Bereiche, Schwerpunkte lassen sich nicht ausmachen.

Trotz der gestiegenen Verfahrenszahlen ist es der Datenschutzbehörde gelungen, fast alle Verfahren in der gesetzlich vorgesehenen Frist von sechs Monaten zu beenden.

### 5.3.2. Grenzüberschreitende Zusammenarbeit

Die bisherige Zusammenarbeit mit anderen Partnerbehörden funktioniert sehr gut. Im Berichtszeitraum wurde erst in wenigen Fällen von der federführenden Aufsichtsbehörde ein Beschlussentwurf vorgelegt (d.h. ein Vorschlag, wie das Verfahren beendet werden sollte).

Wird ein Verfahren bei der Datenschutzbehörde eingebracht und hat die Datenschutzbehörde eine Partnerbehörde nach Art. 60 ff DSGVO einzubeziehen, so setzt die Datenschutzbehörde ihr Verfahren gemäß § 24 Abs. 10 DSG mit Bescheid aus. Sobald feststeht, welche Behörde federführende Aufsichtsbehörde ist bzw. sobald das Verfahren nach Art. 60 DSGVO abgeschlossen ist, erfolgt eine amtswegige Behebung des Aussetzungsbescheides.

### 5.3.3. Verwaltungsstrafverfahren

Im Vergleich zu den Beschwerdeverfahren machen die Verwaltungsstrafverfahren einen geringeren Anteil der anhängigen Verfahren aus.

Ungeachtet dessen sind die Besonderheiten dieses Verfahrens zu beachten.

So war als erster Schritt zu prüfen, ob ein von einer Bezirksverwaltungsbehörde übernommenes Verfahren einzustellen oder fortzuführen war. Einzustellen waren all jene Verfahren, denen ein Verhalten zugrunde lag, welches nach dem 25. Mai 2018 nicht mehr mit Strafe bedroht war (im Wesentlichen betraf dies die Unterlassung einer Meldung an das DVR, strafbar nach § 52 Abs. 2 Z 1 DSG 2000). Hingegen waren alle Verfahren, denen ein Verhalten zugrunde lag, das auch nach dem 25. Mai 2018 allgemein mit Strafe bedroht war, fortzuführen; diese Verfahren

waren allerdings nach dem Günstigkeitsprinzip fortzuführen, d.h. es darf keine höhere Strafe als nach dem DSG 2000 verhängt werden.

Die bisherige Erfahrung zeigt, dass die überwiegende Mehrheit der Verwaltungsstrafverfahren eine behauptete unzulässige Bildverarbeitung nach §§ 12 und 13 DSG (vormals „Videoüberwachung“) zum Gegenstand hat. Die erste – und bisher höchste – Geldstrafe, die deswegen verhängt wurde, beläuft sich auf 4.800 Euro (nicht rechtskräftig).

§ 30 DSG normiert die verwaltungsstrafrechtliche Verantwortlichkeit einer juristischen Person. Demnach kann eine Geldstrafe direkt gegen eine juristische Person verhängt werden und es muss dies nicht im Umweg über den Verantwortlichen nach § 9 VStG erfolgen. Die direkte Strafbarkeit einer juristischen Person ist im VStG – welches im Gegensatz zum Verbandsverantwortlichkeitsgesetz (VbVG) im Bereich der gerichtlich strafbaren Handlungen nur die Strafbarkeit natürlicher Personen kennt –nur unzureichend abgebildet. So ist bspw. unklar, wie der Vertreter einer juristischen Person, zu behandeln ist. Da sich die Verfolgungshandlung nicht gegen ihn, sondern gegen die juristische Person richtet, ist er nicht Beschuldigter. Als Vertreter ist er aber auch nicht Zeuge und kann deshalb nicht unter Wahrheitspflicht einvernommen werden. In analoger Anwendung von § 17 VbVG werden Vertreter beschuldigter juristischer Personen von der Datenschutzbehörde als „Beschuldigte“ vernommen, weil ihnen in dieser Eigenschaft mehr Rechte (v.a. das Verbot der Selbstbezichtigung, das Recht einen Beistand beizuziehen) zukommen. Die Datenschutzbehörde vertritt daher die Ansicht, dass die unmittelbare Strafbarkeit einer juristischen Person im VStG stärker berücksichtigt werden müsste, zumal Regelungen wie in § 30 DSG auch in anderen Materiengesetzen vorgesehen sind (bspw. § 99d BWG, § 26 Abs. 4 NISG uvm.).

Eine weitere Herausforderung stellt die Abgrenzung zwischen DSGVO und VStG dar. Die Führung von Verwaltungsstrafverfahren richtet sich nach dem VStG, jedoch enthält Art. 83 DSGVO einige verfahrensrechtliche Bestimmungen, die im Kollisionsfall dem VStG vorgehen, wie etwa

- Parameter für die Strafbemessung (Art. 83 Abs. 2 DSGVO, § 19 VStG)
- Zusammentreffen strafbarer Handlungen (Absorptionsprinzip nach Art. 83 Abs. 3 DSGVO, Kumulationsprinzip nach § 22 VStG)
- Ermessen der Behörde, ob eine Verwarnung ausgesprochen oder eine Geldstrafe verhängt wird (Art. 83 Abs. 2 DSGVO, § 45 Abs. 1 sowie – seit 1. Jänner 2019 - § 33a VStG)

### 5.3.4. Genehmigung von Verhaltensregeln

Im Berichtszeitraum wurden 7 Anträge auf Genehmigung von Verhaltensregeln eingereicht, ein Antrag wurde (teilweise) bewilligt.

Die niedrige Anzahl der eingereichten Anträge deckt sich aus Sicht der Datenschutzbehörde nicht mit dem im Vorfeld des 25. Mai 2018 angekündigten Interesse an diesem Instrument. Verhaltensregeln können einen Mehrwert für Betroffene und Verantwortliche/Auftragsverarbeiter in einem bestimmten Bereich bilden, weshalb die Ausarbeitung und Einreichung von Verhaltensregeln seitens der Datenschutzbehörde jedenfalls befürwortet wird.

### 5.3.5. Meldungen von Verletzungen des Schutzes personenbezogener Daten

Die Meldepflicht nach Art. 33 DSGVO wird – das zeigen die Verfahrenszahlen – ernst genommen. Die Inhalte der Meldungen variieren stark. Sie reichen vom brieflichen Versenden eines Dokuments an einen falschen Empfänger über den Verlust eines mobilen Endgerätes bis hin zum systematischen Hackerangriff. In den meisten Fällen kann eine zeitnahe Verfahrenseinstellung erfolgen, weil die Meldungsleger alle erforderlichen Abhilfemaßnahmen getroffen haben. Lediglich in zwei Fällen musste die Datenschutzbehörde mit Bescheid auftragen, dass Betroffene von dem Vorfall zu informieren sind.

### 5.3.6. Gescheiterte Novellierung des Grundrechts auf Datenschutz

§ 1 DSG entspricht nach wie vor § 1 DSG 2000. Dies bedingt, dass das Grundrecht auf Datenschutz – anders als die DSGVO – auch für juristische Personen gilt.

Aufgrund des mehrmaligen Scheiterns legistischer Lösungsansätze war die Datenschutzbehörde gezwungen, zum Verhältnis von § 1 DSG (2000) zur DSGVO Stellung zu nehmen.

Dabei kristallisierte sich folgender Lösungsansatz heraus:

§ 1 DSG als verfassungsgesetzlich gewährleistetes Recht schützt juristische Personen ebenso wie natürliche. Dies bedingt, dass juristische Personen aus verfassungsrechtlichen Gründen (vor allem im Hinblick auf den Gleichheitsgrundsatz und die Judikatur des EGMR zu Art. 8 EMRK ) keine unnötige Schmälerung ihrer Rechte dulden sollten. Demnach müssen die einfachgesetzlichen Bestimmungen des DSG (insbesondere § 4 sowie §§ 36 ff) verfassungskonform interpretiert werden.

Eine verfassungskonforme Interpretation führt dazu, dass juristischen Personen jedenfalls die in § 1 DSG normierten Rechte zukommen, nicht aber jene Rechte, die nur in der DSGVO, nicht aber in § 1 DSG Deckung finden (wie bspw. das Recht auf Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit).

Konkret bedeutet dies, dass sich juristische Personen wegen einer behaupteten Verletzung in den Rechten auf Geheimhaltung (§ 1 Abs. 1 DSG), Auskunft (§ 1 Abs. 3 Z 1 leg. cit.), Richtigstellung und Löschung (§ 1 Abs. 3 Z 2 leg. cit.) auf das Grundrecht auf Datenschutz berufen und dieses vor der Datenschutzbehörde geltend machen können.

Bei diesem Lösungsansatz, der bis dato noch keiner gerichtlichen Überprüfung zugeführt wurde, ist zusätzlich zu berücksichtigen, ob es sich um einen „Binnenfall“ oder einen grenzüberschreitenden Fall handelt.

Nach der Rechtsprechung der Datenschutzbehörde kann sich eine juristische Person lediglich in Binnenfällen – d.h. Beschwerdeführer und Beschwerdegegner sind in Österreich und die Datenschutzbehörde ist alleine für das Verfahren zuständig – auf die in § 1 DSG statuierten verfassungsgesetzlichen Rechte berufen (Bescheid vom 13. September 2018, GZ DSB-D216.713/0006-DSB/2018.

Hingegen ist bei grenzüberschreitenden Fällen, wo die federführende Zuständigkeit einer anderen Aufsichtsbehörde im Raum steht und wo die Rechtsfrage ausschließlich auf Basis der DSGVO zu entscheiden ist, die Berufung einer juristischen Person auf § 1 DSG nicht möglich, sodass sie auch keine Rechtsverletzung geltend machen kann (Bescheid vom 19. Juli 2018, GZ DSB-D123.089/0002-DSB/2018). In diesen Fällen kann eine juristische Person – der Rechtsprechung des EuGH folgend – Rechte nur dann geltend machen, wenn sich in der Firma der Name einer natürlichen Person findet (Urteil vom 9. November 2010, C-92/09 und C-093/09).

Diese komplexe Lösung ist im Ergebnis aber nur schwer vermittelbar. Die Datenschutzbehörde hofft daher, dass der Gesetzgeber § 1 DSG novelliert und auf natürliche Personen einschränken wird.

## 5.4. Legistische Umsetzung im Zusammenhang mit der Datenschutz-Folgenabschätzung gem. Art. 35 Abs. 4 und 5 DSGVO

### I. Einleitung

#### 5.4.1. Unionsrechtliche Vorgaben und innerstaatliche Umsetzung

Art. 35 Abs. 1 DSGVO erlegt allen Verantwortlichen die Pflicht auf, eine Datenschutz-Folgenabschätzung (im Folgenden: DSFA) durchzuführen, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen zu rechnen ist.

Eine DSFA ist ein Verfahren, anhand dessen die Verarbeitung beschrieben, ihre Notwendigkeit und Verhältnismäßigkeit bewertet und die Risiken für die Rechte und Freiheiten natürlicher Personen, die die Verarbeitung personenbezogener Daten mit sich bringt, durch eine entsprechende Risikoabschätzung und die Ermittlung von Gegenmaßnahmen kontrolliert werden sollen. Datenschutz-Folgenabschätzungen sind bedeutende Rechenschaftsinstrumente: Verantwortliche können damit nicht nur die DSGVO-Anforderungen besser erfüllen, sondern auch nachweisen, dass geeignete Maßnahmen zur Einhaltung der Verordnung ergriffen wurden. Das heißt also, dass eine DSFA ein Verfahren zur Sicherstellung und zum Nachweis der Einhaltung gesetzlicher Anforderungen ist.

Gemäß der DSGVO können bei Nichteinhaltung der DSFA-Anforderungen von der zuständigen Aufsichtsbehörde Bußgelder verhängt werden. Für den Fall, dass keine DSFA durchgeführt wird, obwohl für die Verarbeitung eine solche erforderlich ist (Art. 35 Abs. 1, 3 und 4), dass eine DSFA nicht ordnungsgemäß durchgeführt wird (Art. 35 Abs. 2 und 7 bis 9) oder dass die zuständige Aufsichtsbehörde – obwohl vorgeschrieben – nicht konsultiert wird (Art. 36 Abs. 3 lit. e), kann ein Bußgeld von bis zu 10 Mio. EUR oder, bei einem Unternehmen, von bis zu 2 % des jährlichen weltweiten Gesamtumsatzes des abgelaufenen Geschäftsjahrs verhängt werden, wobei der höhere der beiden Beträge maßgeblich ist.

Entsprechend dem risikobasierten Ansatz der DSGVO ist eine DSFA nicht für alle Verarbeitungsvorgänge obligatorisch. Eine DSFA ist nur dann erforderlich, wenn eine Form der Verarbeitung „wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt“ (Art. 35 Abs. 1).

Gemäß Art. 35 Abs. 4 DSGVO hat die Aufsichtsbehörde eine Liste der Arten von Verarbeitungsvorgängen zu erstellen und zu veröffentlichen, für die eine DSFA gemäß Abs. 1 durchzuführen ist und kann die Aufsichtsbehörde gemäß Abs. 5 leg. cit. eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine DSFA erforderlich ist.

§ 18 DSG bestimmt die Datenschutzbehörde als nationale Aufsichtsbehörde nach der DSGVO und überträgt ihr gemäß § 21 Abs. 2 die Kompetenz, die Listen nach Art. 35 Abs. 4 und Abs. 5 DSGVO zu erstellen und im Wege einer Verordnung im Bundesgesetzblatt kundzumachen.

Mit der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl. II Nr. 108/2018, hat die Datenschutzbehörde von der (Verordnungs-)Ermächtigung nach Art. 35 Abs. 5 DSGVO in Verbindung mit § 21 Abs. 2 DSG Gebrauch gemacht, und ist die Datenschutzbehörde mit der, am 11.10.2018 in Kraft getretenen, Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-

Folgenabschätzung durchzuführen ist (DSFA-V), BGBl. II Nr. 278/2018, ihrer Verpflichtung aus der DSGVO nachgekommen.

### 5.4.2. Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl. II Nr. 108/2018 (in Kraft getreten am 25.05.2018)

Bei den in der in der Verordnung aufgelisteten Vorbereitungsvorgänge sind all jene Vorgänge umfasst, bei denen nicht vom Vorliegen eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen auszugehen ist.

Dies betrifft folgende Verarbeitungsvorgänge:
All jene – in der Anlage zur Verordnung – genannten Datenverarbeitungen (§ 1 Abs. 1).

Nach § 1 Abs. 2 Z 1 und Z 2 werden von der verpflichtend durchzuführenden DSFA jene Datenanwendungen ausgenommen, die vor dem 24.05.2018 nach den Bestimmungen des § 18 Abs. 2 und § 50c Abs. 1 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013, einer Prüfung (Vorabkontrolle) durch die Datenschutzbehörde unterlagen und im Datenverarbeitungsregister registriert wurden, sowie jene die gemäß § 17 Abs. 2 Z 6 DSG 2000 nicht meldepflichtig waren, sofern diese Datenanwendungen mit Ablauf des 24. Mai 2018 den Vorgaben der DSGVO entsprechen und ab dem Inkrafttreten dieser Verordnung keine wesentlichen Änderungen vorgenommen werden.

Abs. 2 Z 1 fußt auf Erwägungsgrund 171 DSGVO, wonach Genehmigungen der Aufsichtsbehörde in Kraft bleiben, bis sie geändert, ersetzt oder aufgehoben werden. Z 1 stellt klar, dass jene Datenanwendungen, die vor dem 25. Mai 2018 nach Durchführung einer Vorabkontrolle von der Datenschutzbehörde im Datenverarbeitungsregister registriert wurden, ebenfalls keiner Datenschutz-Folgenabschätzung unterliegen. Datenanwendungen, die der Vorabkontrolle unterlagen, wurden vor ihrer Registrierung einem Prüfverfahren unterzogen, ob sie mit datenschutzrechtlichen Vorgaben im Einklang stehen. Nur wenn diese Art der Datenverarbeitung zulässig war, erfolgte eine Registrierung im Datenverarbeitungsregister, gegebenenfalls unter Auflagen. War dies nicht der Fall, erfolgte eine (bescheidmäßige) Ablehnung. Es ist daher angebracht, die im Rahmen einer Vorabkontrolle geprüften Datenanwendungen von einer DSFA auszunehmen, weil die datenschutzkonforme Verarbeitung durch die Registrierung bestätigt wurde, was einer Genehmigung gleichgehalten werden kann (siehe dazu auch die Ausführungen in den von der Gruppe nach Art. 29 der Richtlinie 95/46/EG - Datenschutz-Richtlinie angenommenen „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP 248 Rev.01 vom 4. April 2017).

Abs. 2 Z 2 fußt inhaltlich auf der (mit Ablauf des 24. Mai 2018 außer Kraft getretenen) Standard- und Musterverordnung 2004 (StMV), BGBl. II Nr. 312. Ein inhaltliches Aufbauen auf der StMV schien insofern geboten, als diese Datenanwendungen beinhaltet, bei denen von einer Gefährdung schutzwürdiger Geheimhaltungsinteressen von Betroffenen nicht auszugehen ist, da der Verordnungsgeber von einem geringen Risiko für die Rechte und Freiheiten natürlicher Personen ausging, weshalb es angemessen erschien, auch diese Datenanwendungen von der Pflicht zur Durchführung einer DSFA auszunehmen.

Die Verordnung sowie die Erläuterungen sind auf der Website der Datenschutzbehörde abrufbar.

### 5.4.3. Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl. II Nr. 278/2018 (in Kraft getreten am 10.11.2018)

Nach der DSGVO müssen die Verantwortlichen geeignete Maßnahmen ergreifen, um sicherzustellen – und den Nachweis dafür zu erbringen –, dass die Verarbeitung gemäß der DSGVO erfolgt, wobei sie unter anderem die „unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen" zu berücksichtigen haben. Die

Vorgabe, dass die/der Verantwortliche unter bestimmten Voraussetzungen eine DSFA durchführen muss, ist vor dem Hintergrund ihrer allgemeinen Pflicht zu verstehen, eine geeignete Abschätzung der Risiken zu betreiben, welche die Verarbeitung personenbezogener Daten birgt.

Mit der DSFA-V sollen Verantwortliche in ihrer Verpflichtung dahingehend unterstützt werden, dass Verarbeitungsvorgänge normiert werden, bei denen vom Vorliegen eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen jedenfalls auszugehen ist und die folglich der Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung unterliegen. Dies bedeutet jedoch nicht, dass Verarbeitungsvorgänge, die von dieser Verordnung nicht erfasst sind, keiner Pflicht zur Durchführung einer DSFA unterliegen. Bei Verarbeitungsvorgängen, die weder von dieser Verordnung, noch von der DSFA-AV erfasst sind, ist daher zu prüfen, ob eine Datenschutz-Folgenabschätzung erforderlich ist oder nicht.

Die Datenschutzbehörde hat dabei die Vorgabe des Art. 35 Abs. 4 DSGVO, wonach die Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge zu erstellen hat, für die eine DSFA durchzuführen ist, nicht dahingehend interpretiert, eine abschließende Aufzählung vorzunehmen, sondern wurden im Wege eines Kriterienkatalogs jene Verarbeitungsvorgänge normiert, bei denen vom Vorliegen eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen jedenfalls auszugehen ist und die folglich der Verpflichtung zur Durchführung einer DSFA unterliegen. Dabei hat sie sich insbesondere an den (neun) Kriterien der „Leitlinien des Europäischen Datenschutzausschusses zur Datenschutz-Folgenabschätzung“, 17/DE WP 248“ orientiert und diese unter Berücksichtigung der Vorgaben in Art. 35 Abs. 3 DSGVO konkretisiert. Die von der Arbeitsgruppe in den Leitlinien getroffene Feststellung, wonach es in einigen Fällen (jedoch) vorkommen kann, dass ein für die Datenverarbeitung Verantwortlicher von der Notwendigkeit einer DSFA ausgehen muss, obwohl der fragliche Verarbeitungsvorgang nur eines dieser (Anm: in den Leitlinien genannten) Kriterien erfüllt, wurde in den Kriterienkatalog der Verordnung insoweit übernommen, als bei den in § 2 Abs. 2 genannten Fällen eine DSFA durchzuführen ist, wenn zumindest ein in Z 1 bis Z 6 genanntes Kriterium erfüllt ist. Bei den in Abs.3 genannten Kriterien ist eine DSFA hingegen obligatorisch, wenn ein Verarbeitungsvorgang zwei oder mehr der in Z 1 bis Z 5 genannten Kriterien erfüllt.

Vom Geltungsbereich ausgenommen wurden Verarbeitungsvorgänge nach dem 3. Hauptstück des DSG (§§ 36 ff; Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs).

Unter Anwendung des Kohärenzverfahrens im Sinne des Art. 35 Abs. 6 iVm Art. 63 DSGVO und Übermittlung an den Europäischen Datenschutzausschuss erfolgte eine Überarbeitung, mit welchen den Empfehlungen des Ausschusses Rechnung getragen wurde und konnte die Verordnung sodann im Bundesgesetzblatt kundgemacht werden.

Die Verordnung und die Erläuterungen sind auf der Website der Datenschutzbehörde abrufbar.

# 6 Europäische Zusammenarbeit

## 6.1 Europäische Union

### 6.1.1 Der Europäische Datenschutzausschuss

Mit 25. Mai 2018 wurde die Art. 29-Datenschutzgruppe durch den neu geschaffenen Europäischen Datenschutzausschuss (EDSA) abgelöst.

Diese unabhängige, mit eigener Rechtspersönlichkeit ausgestattete und aus Vertretern der Aufsichtsbehörden des EWR bestehende europäische Einrichtung wurde dabei mit weitreichenden Kompetenzen ausgestattet. War die Art. 29-Datenschutzgruppe als Beratungsgremium der Europäischen Kommission, erarbeitet der EDSA nunmehr nicht nur Leitlinien und Empfehlungen zu datenschutzrechtlichen Fragestellungen (Art. 70 DSGVO), sondern kann auch gemäß Art. 64 DSGVO Stellungnahmen und gemäß Art. 65 DSGVO verbindliche Beschlüsse im Kohärenzverfahren abgeben.

2018 hat der EDSA zu 27 nationalen Listen über Verarbeitungstätigkeiten, die einer Datenschutz-Folgenabschätzung unterliegen, Stellungnahmen gemäß Art. 64 DSGVO abgegeben.

Zudem hat der EDSA 2018 zu folgenden Themen Leitlinien angenommen und veröffentlicht (https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en):

- Akkreditierung von Zertifizierungsstellen nach der DSGVO (EDPB Guidelines 4/2018) [Annex 1 befindet sich zu Redaktionsschluss des Berichtes noch im öffentlichen Konsultationsverfahren]
- Territorialer Anwendungsbereich der DSGVO (Art. 3) (EDPB Guidelines 3/2018) [befindet sich zu Redaktionsschluss des Berichtes im öffentlichen Konsultationsverfahren]
- Ausnahmeregelungen des Art. 49 DSGVO (EDPB Guidelines 2/2018)
- Zertifizierung und Identifikation von Zertifizierungskriterien gemäß Art. 42 und 43 DSGVO (EDPB Guidelines 1/2018) [befindet sich derzeit noch im öffentlichen Konsultationsverfahren]

Folgende in Vorbereitung auf die DSGVO zu Redaktionsschluss des Berichtes von der Art. 29-Datenschutzgruppe erarbeiteten Leitlinien, Empfehlungen, Positions- und Arbeitspapiere wurden vom EDSA am 25. Mai 2018 bestätigt (https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en):

- Leilinien in Bezug auf die Einwilligung nach der DSGVO (WP259 rev.01)
- Leitlinien zur Transparenz (WP260 rev.01)
- Leitlinien zur automatisierten Entscheidungsfindung im Einzelfall und Profiling (WP251rev.01)
- Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten (WP250 rev.01)
- Leitlinien zum Recht auf Datenübertragbarkeit (WP242 rev.01)
- Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der DSGVO „wahrscheinlich ein hohes Risikomit sich bringt“ (WP248 rev.01)
- Leitlinien zum Datenschutzbeauftragten (WP243 rev.01)
- Leitlinien zur Identifizierung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters (WP244 rev.01)
- Positionspapier zu Ausnahmen von der Verpflichtung gemäß Art. 30(5) DSGVO, ein

Verzeichnis von Verarbeitungstätigkeiten zu führen
- Arbeitsdokument zur Festlegung eines Kooperationsverfahrens für die Genehmigung von BCRs für Verantwortliche und Auftragsverarbeiter im Rahmen der GDPR (WP 263 rev.01)
- Empfehlung zum Standardantrag auf Genehmigung von BCRs des Verantwortlichen für die Übermittlung personenbezogener Daten (WP 264)
- Empfehlung zum Standardantrag auf Genehmigung von BCRs des Auftragsverarbeiters für die Übermittlung personenbezogener Daten (WP 265)
- Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher interner Datenschutzvorschriften (BCR) (WP 256 rev.01)
- Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher interner Datenschutzvorschriften (BCR) für Auftragsverarbeiter (WP 257 rev.01)
- Referenzgrundlage für die Angemessenheit (WP 254 rev.01)
- Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der DSGVO (WP 253)

Die Arbeit des EDSA, wie etwa Stellungnahmen, Leitlinien und Empfehlungen, wird durch Expertenuntergruppen mit jeweiligem Fachpersonal der Aufsichtsbehörden auf dem entsprechenden Gebiet vorbereitet. Im Jahr 2018 wurden zwei neue Untergruppen geschaffen, nämlich die Social Media Expertenuntergruppe und die IT Users Expertenuntergruppe.

Die Social Media Expertenuntergruppe befasst sich mit der Analyse der Funktionen von Social Media, einschließlich der zugrundeliegenden Verarbeitungsaktivitäten und der entsprechenden Risiken für die Rechte und Freiheiten des Einzelnen, gibt Anleitung betreffend das Angebot und auch auf die Nutzung von Social Media-Funktionen, insbesondere aus wirtschaftlichen oder politischen Gründen und unterstützt alle anderen Expertenuntergruppen in diesem Bereich.

Die IT Users Expertenuntergruppe entwickelt und testet die für die grenzüberschreitende Zusammenarbeit eingerichtete Internetplattform praxisnah und stellt die übrige technische Infrastruktur des EDSA sicher (etwa Tele- und Videokonferenzsysteme).

Zudem verfügt der Datenschutzausschuss noch über folgende Untergruppen:

Die BTLE (Border Travel and Law Enforcement) Expertenuntergruppe befasst sich mit der Strafverfolgungsrichtlinie, den Vorschlägen zu e-Evidence, Art. 48 DSGVO, PNR-Daten, dem Datenzugriff seitens nationaler Nachrichtendiensten sowie der Vorbereitung der koordinierten Aufsicht nach Art. 62 EU VO 45/2001.

Die Cooperation Expertenuntergruppe legt einen generellen Fokus auf Verfahrensfragen der grenzüberschreitenden Kooperation von Aufsichtsbehörden nach der DSGVO und erarbeitet in diesem Sinne Anleitungen zu Art. 56 Abs. 2 bis 5 DSGVO, Kapitel 7 Abschnitt 1 und 2 DSGVO, zu Kooperationsfällen, bei welchen es keine Niederlassung in der EU gibt sowie zu internationalen Kooperationen nach Art. 50 DSGVO.

Die Compliance, e-Government und Health Expertengruppe (frühere e-Government Untergruppe) befasst sich mit Verhaltensregeln, Zertifizierungs- und Akkreditierungsprozessen sowie datenschutzrechtlichen Fragen im Zusammenhang mit den Themen e-Government und Gesundheit.

Die Enforcement Expertengruppe beschäftigt sich mit praktischen Fragen von Ermittlungsaktivitäten und Untersuchungen der Aufsichtsbehörden, entwickelt eine Enforcement-Strategie

und arbeitet gemeinsam mit der Fining Task Force an Leitlinien zur Anwendung von Kapitel 8 DSGVO.

Die Financial Matters Expertengruppe legt ihren Fokus auf datenschutzrechtliche Fragestellungen im Finanzsektor (z.B. FATCA, automatischer Austausch von Daten zu Steuerzwecken und Geldwäschebekämpfung).

Die Fining Task Force arbeitet an der Entwicklung von Leitlinien zur Harmonisierung der Berechnung von Geldbußen nach der DSGVO.

Die Strategic Advisory Expertenuntergruppe beschäftigt sich mit strategischen Fragen des gesamten Ausschusses und versucht Fragen zu klären, die auf Ebene der anderen Expertengruppen nicht gelöst werden können.

Die ITS (International Transfer) Expertenuntergruppe erarbeitet Anleitungen zu Fragen des internationalen Transfers von personenbezogenen Daten nach Kapitel V DSGVO. Dabei befasst sich diese Untergruppe insbesondere mit der Überprüfung von Angemessenheitsentscheidungen der Europäischen Kommission (wie etwa dem Privacy Shield), Verhaltensregeln und Zertifizierungen als Transferinstrumente und mit dem Austausch der Behörde zu Überprüfungen von BCRs und Ad-Hoch-Vertragsklauseln nach Art. 46 DSGVO.

Die Key Provisions Expertenuntergruppe arbeitet an Leitlinien zu Grundbegriffen und Kernkonzepten des Kapitel 1 (Anwendungsbereich und Definitionen der DSGVO), 2 (Grundsätze), 3 (z.B. Rechte des Einzelnen, Transparenz), 4 (z.B. DPO) und 9 DSGVO.

Die Technology Expertenuntergruppe beschäftigt sich mit Technologien sowie Innovationen und den damit verbundenen Herausforderungen für den Datenschutz, einschließlich ePrivacy. In diesem Sinne unterstützt diese Expertenuntergruppe alle anderen Gruppen mit ihrem technischen Knowhow.

Unterstützt wird der EDSA, samt dem Plenum und der Expertenuntergruppen, durch ein eigenes Sekretariat, das sowohl technische und administrative als auch juristische Unterstützung bietet.

Der EDSA hat sich seit dem 25. Mai 2018 bis Ende 2018 fünfmal zu Plenarsitzungen getroffen. Für 2019 sind insgesamt 11 Plenarsitzungen geplant. Die diesbezüglichen Tagesordnungen und Presseaussendungen sind, wie viele andere Informationen zur Arbeit des EDSA, auf der Website des EDSA unter https://edpb.europa.eu/ zu finden.

### 6.1.2 Europol

Das Europäische Polizeiamt (Europol) ist eine europäische Polizeibehörde mit der Aufgabe, die Leistungsfähigkeit der zuständigen Behörden der Mitgliedstaaten und ihre Zusammenarbeit im Hinblick auf die Verhütung und die Bekämpfung des Terrorismus, des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität zu verbessern. Europol verarbeitet zu diesem Zweck große Mengen von vor allem strafrechtsrelevanten Daten. Diese Verarbeitung unterlag bis Mai 2017 der besonderen Kontrolle durch eine gemeinsame Kontrollinstanz, die aus Vertretern aller EU Datenschutzbehörden bestand, dem „Europol Joint Supervisory Body“ (JSB). Mit der neuen Europol Verordnung [10] 794/2016 vom 11. Mai 2016, die am 01.Mai 2017 in Kraft trat, wurde diese gemeinsame Kontrollinstanz abgeschafft. An ihre Stelle

10 http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0794&from=EN

trat eine aufgeteilte Kontrolle: Einerseits durch nationale Kontrollinstanzen, die die Zulässigkeit der Eingabe und des Abrufs personenbezogener Daten sowie jedweder Übermittlung dieser Daten an Europol überwachen, und andererseits durch den europäischen Datenschutzbeauftragten (EDPS), der die Verarbeitung durch Europol überwacht. Jede betroffene Person kann beim Europäischen Datenschutzbeauftragten eine Beschwerde einreichen, wenn sie der Ansicht ist, dass Europol bei der Verarbeitung ihrer personenbezogenen Daten gegen die Europol-Verordnung verstößt. Darüber hinaus kann jede Person die nationale Kontrollbehörde ersuchen, die Rechtmäßigkeit jeglicher Übermittlung ihrer personenbezogenen Daten an Europol sowie die Verarbeitung dieser Daten durch den betreffenden Mitgliedstaat zu prüfen. Die Vertreter der nationalen Kontrollbehörde der Mitgliedstaaten und der Europäische Datenschutzbeauftragte bilden gemeinsam den Beirat für Zusammenarbeit. Die Hauptaufgabe des Beirates ist es, sich mit den allgemeinen Richtlinien und Strategien von Europol im Bereich der Überwachung des Datenschutzes sowie der Zulässigkeit der Verarbeitung und die Übermittlung von personenbezogenen Daten an Europol auseinanderzusetzen.

### 6.1.3 Schengen

Das Schengener Informationssystem der zweiten Generation (kurz „SIS II“) ermöglicht nationalen Grenz-, Zoll-, Visa- und Strafverfolgungsbehörden Fahndungen zu gesuchten oder vermissten Personen bzw. gestohlenen oder verlorenen Sachen, insbesondere Dokumente und Fahrzeuge, im Schengen-Raum auszuschreiben bzw. abzufragen. Die Rechtsgrundlage für das SIS II bildet die sogenannte SIS-II-Verordnung.[11] Das SIS II besteht aus einem zentralen System (C.SIS), den jeweiligen nationalen Systemen der Mitgliedstaaten (N.SIS II) sowie einer Kommunikationsinfrastruktur zwischen dem zentralen System und den nationalen Systemen. Das österreichische N.SIS II wird vom Bundesministerium für Inneres als Verantwortlicher geführt. Die jeweiligen nationalen Datenschutzbehörden haben gemäß der SIS-II-Verordnung die Rechtmäßigkeit der Verarbeitung personenbezogener SIS-II-Daten auf nationaler Ebene zu überwachen. Darüber hinaus haben die nationalen Datenschutzbehörden mindestens alle vier Jahre die Datenverarbeitungsvorgänge im N. SIS II nach internationalen Prüfungsstandards zu überprüfen. Die Europäische Kommission überprüft gemeinsam mit nationalen Experten die Umsetzung der SIS-II-Verordnung in den einzelnen Mitgliedsaaten. Im Berichtszeitraum haben Mitarbeiter der Datenschutzbehörde an Evaluierungen in Irland und Estland teilgenommen. Die Datenschutzbehörde wird sich auch im Jahr 2019 an Evaluierungen beteiligen.

### 6.1.4 Zoll

Das gemeinsame Zollinformationssystem (ZIS) dient der Erfassung von Daten von Waren, Transportmittel, natürlichen und juristischen Personen, die im Zusammenhang mit Verstößen gegen das gemeinsame Zoll- und Agrarrecht stehen. Das ZIS ermöglicht einem Mitgliedstaat, der Daten in das System eingegeben hat, einen ZIS-Partner in einem anderen Mitgliedstaat um die Durchführung u.a. gezielter Kontrollen zu ersuchen. Zur Gewährleistung eines angemessenen Datenschutzes wurde neben dem Ausschuss gemäß Art. 43 der ZIS-Verordnung[12] („Joint Supervisory Authority of Customs“ („JSA“)) eine Koordinierende Aufsichtsbehörde (CIS Supervision Coordination Group („CIS-SCG“)) eingerichtet, welche aus Vertretern der nationalen Datenschutzbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten gebildet wird. Im Berichtszeitraum fanden zwei Sitzungen des JSA bzw. der CIS-SCG statt.

### 6.1.5 Eurodac

Das „Eurodac“-System ermöglicht den Einwanderungsbehörden der Mitgliedstaaten Asylwerber und andere Personen zu identifizieren, die beim illegalen Überschreiten einer EU-Außengrenze aufgegriffen werden. Anhand der Fingerabdrücke kann ein Mitgliedstaat feststellen, ob ein Fremder in einem anderen Mitgliedstaat Asyl beantragt hat oder ob ein Asylwerber illegal in

11 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32006R1987
12 http://eur-lex.europa.eu/legal-content/dE/TXT/?uri=celex:31997R0515

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

### 6.1.6 Visa

Das Visa-Informationssystem (VIS) enthält Daten zu Ausstellungen, Ablehnungen, Annullierungen, Widerrufen und Verlängerungen von Kurzzeit-Visa in den Mitgliedstaaten des Schengen Raums. Die rechtliche Grundlage für das VIS bildet die Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Einrichtung des Visa-Informationssystems (VIS-Verordnung). Das VIS besteht aus einem zentralen Visa-Informationssystem (C-VIS), einem nationalen System (N-VIS) in jedem Mitgliedstaat und aus einer Kommunikationsinfrastruktur zwischen dem zentralen Visa-Informationssystem und den nationalen Systemen. Die nationale VIS-Stelle in Österreich ist das Bundesministerium für Inneres. Die jeweiligen nationalen Datenschutzbehörden haben gemäß der VIS-Verordnung die Rechtmäßigkeit der Verarbeitung personenbezogener VIS-Daten auf nationaler Ebene zu überwachen. Darüber hinaus haben die nationalen Datenschutzbehörden mindestens alle vier Jahre die Datenverarbeitungsvorgänge im N.VIS nach internationalen Prüfungsstandards zu überprüfen. Die Datenschutzbehörde hat im Berichtszeitraum an der VIS-User-Konferenz in Kairo teilgenommen.

### 6.1.7 Gemeinsame Stellungnahme der SIS II, VIS und Eurodac Koordinierungsgruppen- zur Interoperabilität zwischen EU-Informationssystemen

Die Koordinierungsgruppen des SIS II, VIS und Eurodac haben im Juni 2018 eine gemeinsame Stellungnahme [14] an das Europäische Parlament, den Rat sowie die Europäische Kommission zu den beiden Verordnungsentwürfen der Europäischen Kommission vom 12. Dezember 2017 zur Interoperabilität zwischen EU-Informationssystemen[15] übermittelt. Die Verordnungsentwürfe der Europäischen Kommission sehen nicht nur die Vernetzung der bestehenden europäischen Großinformationssysteme SIS II, VIS und Eurodac sowie der künftigen Systeme EES, ETIAS und ECRIS-TCN vor, sondern auch die Schaffung sekundärer, biometrischer Datenbanken sowie eine Erweiterung der bestehenden Zugriffsrechte. Die Koordinierungsgruppen äußerten in der Stellungnahme ihre datenschutzrechtlichen Bedenken gegenüber den beiden Verordnungsentwürfen und empfahlen entsprechende Gesetzesänderungen.

### 6.1.8. Europarat

Die Datenschutzbehörde vertritt die Republik Österreich im Ausschuss nach Art. 18 (T-PD) der Datenschutzkonvention des Europarates (EVS Nr. 108; BGBl. Nr. 317/1988). Im Berichtszeitraum fanden von 19. bis 21. Juni die 36. Plenarsitzung und von 20. Bis 22. November 2018 die 37. Plenarsitzung des T-PD in Straßburg statt. Die Tagesordnungen sowie die zusammenfassenden Berichte der Sitzungen sind in englischer Sprache unter https://www.coe.int/en/web/data-protection/consultative-committee-tpd/meetings abrufbar.

---

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

14 https://edps.europa.eu/sites/edp/files/publication/18-06-22_letter_on_interoperability_scgs_ep_en.pdf

15 COM (2017) 793 final, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Grenzen und Visa) und zur Änderung der Entscheidung 2004/512/EG des Rates, der Verordnung (EG) Nr. 767/2008, des Beschlusses 2008/633/JI des Rates, der Verordnung (EU) 2016/399 und der Verordnung (EU) 2017/2226 sowie COM (2017) 794 final, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration).

# 7 Internationale Beziehungen

## Privacy Shield – 2nd Annual Joint Review

Gemäß des am 12. Juli 2016 angenommenen EU-US-Datenschutzschilds („EU-US Privacy Shield") nahmen sieben Vertreter des Europäischen Datenschutzausschusses, darunter auch eine Vertreterin der österreichischen Datenschutzbehörde, an der zweiten gemeinsamen Überprüfung der Angemessenheitsentscheidung durch die Europäische Kommission am 18. und 19. Oktober 2018 in Brüssel teil. Diese jährliche Überprüfung dient dazu, die Robustheit der Angemessenheitsentscheidung und ihrer praktischen Umsetzung zu bewerten.

Ausgehend von vorangegangenen Stellungnahmen der Art. 29 Datenschutzgruppe, insbesondere der Stellungnahme 1/2016, und dem Bericht zur ersten gemeinsamen Überprüfung im Vorjahr, konzentrierte sich der EDSA auf die Bewertung sowohl der kommerziellen Aspekte des Privacy Shields als auch des Zugangs der Regierung zu personenbezogenen Daten, die aus der Europäischen Union zum Zwecke der Strafverfolgung und der nationalen Sicherheit übermittelt wurden, einschließlich der den EU-Bürgern zur Verfügung stehenden Rechtsbehelfe. Hierbei prüfte der EDSA insbesondere, ob diese Bedenken ausgeräumt wurden und ob die im Rahmen des EU-U.S. Privacy Shields gewährten Garantien praktikabel und wirksam sind.

Die Europäische Kommission hat ihren eigenen Bericht über die zweite gemeinsame Überprüfung am 19. Dezember 2018 veröffentlicht.

Die wichtigsten Ergebnisse des EDSA zu dieser zweiten gemeinsamen jährlichen Überprüfung, die sich sowohl aus schriftlichen Eingaben als auch aus mündlichen Beiträgen ergeben, werden im Bericht[16] dazu präzise dargestellt.

Den Schlussfolgerungen des EDSA ist im Wesentlichen zu entnehmen, dass die Bemühungen der US-Behörden und der Kommission zur Umsetzung des Privacy Shields, insbesondere die Maßnahmen zur Anpassung des Erstzertifizierungsverfahrens, zur Einleitung von Aufsichts- und Durchsetzungsmaßnahmen von Amts wegen, sowie die Bemühungen der US-Behörden, mehr Transparenz über die Ausübung von Überwachungsbefugnissen und die Ernennung eines neuen Vorsitzenden sowie zweier neuer Mitglieder des „Privacy and Civil Liberties Oversight Board" (PCLOB) zu erlangen, was bedeutet, dass das PCLOB das für seine Tätigkeit erforderliche Quorum erreicht hat, begrüßt werden. Dennoch hat der EDSA nach wie vor eine Reihe von Bedenken, die sowohl von der Kommission als auch von den US-Behörden ausgeräumt werden müssen.

Einer der größten Kritikpunkte ist die nach wie vor fehlende dauerhafte Besetzung der Ombudsperson – und das, obwohl diese ein Kernstück des Privacy Shields darstellt. Darüber hinaus mangelt es an der Offenlegung ihrer Befugnisse gegenüber den Sicherheitsbehörden. Angesichts der dieses Jahr bei der Überprüfung dargelegten Elemente ist der EDSA nicht in der Lage, zu dem Schluss zu kommen, dass die Ombudsperson über ausreichende Befugnisse verfügt, um Zugang zu Informationen zu erhalten und Verstöße zu beheben und damit bleibt es letztlich nach wie vor zweifelhaft, ob der Ombudspersonmechanismus in der Praxis das erforderliche Maß an Rechtschutz gewährt.

Auch was den Bereich der Sammlung von Daten und den Zugang zu Daten durch die nationalen Sicherheitsbehörden anbelangt, fehlen weiterhin konkrete Zusicherungen seitens der US-Behörden. Hierbei kann der EDSA das PCLOB nur ermutigen, weitere Berichte zu erstellen und zusätzliche Elemente für die Anwendung der Garantien von PPD-28, Abschnitt 702 FISA und Erlass 12333 zu liefern.

16 https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en