Datenschutzfragen in Internet und eCommerce/eBusiness

Hans G. Zeger

Juridicum Wien, VO Sommersemester 2019

Download: http://www.e-monitoring.at/static/vo-ds-internet.pdf

VO SS2019 - Juridicum

Download Vorlesungsunterlagen:

http://www.e-monitoring.at/static/vo-ds-internet.pdf

Dr. Hans G. Zeger
e-commerce monitoring gmbh
A-1010 Wien, Vorlaufstraße 5/6

Tel.:	01 / 53 20 944
Mail persönlich:	hans.zeger@e-monitoring.at
Zertifizierung:	http://www.globaltrust.eu
e-commerce:	http://www.e-monitoring.at

Grundfragen

Was ist überhaupt "Datenschutz"?

- **1890** formulierten Warren/Brandeis in der Harvard Law Review ein "right to be let alone" (The Right to Privacy), gilt als Beginn des modernen Privatsphäregedankens
- **70er**-Jahre europaweit diverse Datenschutzinitiativen als Gegenbewegung zu Entwicklungen in der Computertechnik (inkl. Europarat, OECD)
- **1978** im öDSG Datenschutz als Interpretation des Art. 8 EMRK (Teil des Privat- und Familienlebens), im DSG 2000 beibehalten
- **2009** Datenschutz wird eigenes Grundrecht in EU-Grundrechtecharta
- **1983** deutsches Volkszählungsurteil "informationelles Selbstbestimmungsrecht" (Bundesverfassungsgericht)
- **2008** deutsches Online-Durchsuchungsurteil formuliert "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" (Bundesverfassungsgericht)

"Datenschutz" als moderne Ausformung von Grundrechten

VO SS2019 - Juridicum

Quellen:

- S. D. Warren, L. D. Brandeis, The Right to Privacy, Harvard Law Review Vol. 4, Nr. 5, S192-220
- Datenschutzgesetz [1978] StF: BGBl. Nr. 565/1978
- OECD: RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (23rd September, 1980)
- Europarat: CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA Strasbourg, 28.I.1981 (*ETS 108 – Automatic processing of Personal Data)*
  [BGBl. Nr. 210/1958]
- BVerfGE 65,1 Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83
- Datenschutzgesetz 2000 StF: BGBl. Nr. 165/1999
- BVerG Karlsruhe, Urteil vom 27. Februar 2008 - 1 BvR 370/07; 1 BvR 595/07 – Vorschriften im Verfassungsschutzgesetz NRW zur Online-Durchsuchung und zur Aufklärung des Internet nichtig
- EU-Grundrechtecharta C 83/393 30.3.2010 "Artikel 8 Schutz personenbezogener Daten (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. ..."

Grundfragen

Was ist das Internet?

- technische Infrastruktur ("Unternehmensvernetzung", "virtual private networks", "IP-Telefonie", ...)
- Plattform für wirtschaftliche Tätigkeiten ("eCommerce", "Online-Shops", "Musik-Download", ...)
- Informationsvermittlung ("soziales Medium", "Stammtisch", "sozialer Treffpunkt", ...)
- Erweiterung der Privatsphäre ("eMail", "Weblog"/Tagebuch, "Erweiterung des Freundeskreis", ...)
- politischer Aktionsraum ("Kooperation", "Vernetzung", "Foren", ...)

Abgrenzung nicht immer offensichtlich,
können zu gegensätzlichen Interessen führen

VO SS2019 - Juridicum

-

Anwendungsfälle Datenschutz

Welche (Internet-)Situationen sind überhaupt datenschutzrelevant?

- Nutzung von Informationsdiensten ("Online-Services", "Apps"), personalisiert/"anonym" und/oder kostenpflichtig/"gratis"
- Bestellungen im Internet ("eCommerce", Online-Shop)
- elektronische Amtswege und öffentliche Verwaltung, Vorschreibungen ("eGovernment")
- Selbstdarstellung / Meinungsäußerung ("Web2.0", "Social Media")
- Veröffentlichung persönlicher Daten durch Dritte
- Nutzung als Infrastruktur (virtuelle Unternehmensnetze, Intranet, Extranet)
- Vereinbarung mit dem Provider, Tätigkeit der Provider (z.B Vertraulichkeit des eMail-Verkehrs)
- sonstige Internetnutzungen: ????

VO SS2019 - Juridicum

-

Anwendbare Bestimmungen

Wo finden sich zum Internet datenschutzrelevante Bestimmungen?

- DSGVO + DSG (Verarbeitungsvoraussetzungen, Schutzbestimmungen)
- TKG 2003 (Verarbeitungsvoraussetzungen, Schutzbestimmungen, Auskunftspflichten, Auftragsverarbeiter)
- ABGB Privatsphärebestimmung (Schutzbestimmung)

- SPG (Auskunftspflichten)
- ECG (Auftragsverarbeiter, Haftung, Auskunftspflichten)
- StPO (Auskunftspflichten)
- UrhG (Auskunftspflichten)

- Materiegesetze, wie E-Government Gesetz, Gesundheitstelematikgesetz, Universitätsorganisaitonsgesetz, ...)

VO SS2019 - Juridicum

-

Schutz der Privatsphäre - Übersicht

Bestimmungen zum Schutz der Privatsphäre

- EMRK Art 8 (Privatsphäre, Familienleben, Briefverkehr)
- EU-Grundrechtecharta Art 8 (Datenschutz)
- StGG (Staatsgrundgesetz) Art 9, 10 (Briefgeheimnis) u. 10a (Fernmeldegeheimnis)
- DSGVO, insb. Art 1 (Sicherung der Rechte und Freiheiten)
- § 16 ABGB (angeborene Rechte)
- StGB z.B. § 118 (Briefgeheimnis), § 119 (Telekommunikationsgeheimnis) und §§ 302ff (Amtsmissbrauch), § 107a ("Stalking"), § 107c ("Mobbing")
- TKG 2003 § 93 (Kommunikationsgeheimnis)
- MedienG § 7ff (Bloßstellung)
- UrhG § 77 (Briefe, Tagebücher, ähnliche vertrauliche Aufzeichnungen), § 78 (Bildnissschutz)
- Regelungen für einzelne Berufsgruppen
- ABGB § 1328a (Bloßstellung)

VO SS2019 - Juridicum

Europäische Menschenrechtskonvention

Artikel 8 Recht auf Achtung des Privat- und Familienlebens

(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Charta der Grundrechte der Europäischen Union 26. Oktober 2012

(EU-Grundrechtecharta)

Artikel 8 Schutz personenbezogener Daten

(1) Jede **Person** hat das Recht auf Schutz der sie **betreffenden personenbezogenen Daten**.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer **unabhängigen Stelle überwacht**.

Staatsgrundgesetz vom 21. Dezember 1867

Artikel 9. Das Hausrecht ist unverletzlich. […]

Artikel 10. Das Briefgeheimnis darf nicht verletzt und die Beschlagnahme von Briefen, außer dem Falle einer gesetzlichen Verhaftung oder Haussuchung, nur in Kriegsfällen oder auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze vorgenommen werden.

[BGBl. Nr. 8/1974] Artikel 10a. Das Fernmeldegeheimnis darf nicht verletzt werden. Ausnahmen von der Bestimmung des vorstehenden Absatzes sind nur auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig.

Allgemeines Persönlichkeitsrecht im ABGB

§ 16. Jeder Mensch hat angeborene, schon durch die Vernunft einleuchtende Rechte, und ist daher als eine Person zu betrachten. Sclaverey oder Leibeigenschaft, und die Ausübung einer darauf sich beziehenden Macht, wird in diesen Ländern nicht gestattet.

TKG 2003 – Kommunikationsgeheimnis

§ 93. (1) Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.
(2) Zur Wahrung des Kommunikationsgeheimnisses ist jeder Betreiber eines öffentlichen Kommunikationsnetzes oder -dienstes und alle Personen, die an der Tätigkeit des Betreibers mitwirken, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.
(3) Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung, der Überwachung von Nachrichten, der Auskunft über Daten einer Nachrichtenübermittlung, der Auskunft über Daten nach § 99 Abs. 3a FinStrG und der Auskunft über Daten nach § 11 Abs. 1 Z 7 PStSG sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.
(4) Werden mittels einer Funkanlage, einer Telekommunikationsendeinrichtung oder mittels einer sonstigen technischen Einrichtung Nachrichten unbeabsichtigt empfangen, die für diese Funkanlage, diese Telekommunikationsendeinrichtung oder den Anwender der sonstigen Einrichtung nicht bestimmt sind, so dürfen der Inhalt der Nachrichten sowie die Tatsache ihres Empfanges weder aufgezeichnet noch Unbefugten mitgeteilt oder für irgendwelche Zwecke verwertet werden. Aufgezeichnete Nachrichten sind zu löschen oder auf andere Art zu vernichten.
(5) Das Redaktionsgeheimnis (§ 31 Mediengesetz) sowie sonstige, in anderen Bundesgesetzen normierte Geheimhaltungsverpflichtungen sind nach Maßgabe des Schutzes der geistlichen Amtsverschwiegenheit und von Berufsgeheimnissen sowie das Verbot deren Umgehung gemäß §§ 144 und 157 Abs. 2 StPO zu beachten. Den Anbieter trifft keine entsprechende Prüfpflicht.

Mediengesetz

§ 7. (1) Wird in einem Medium der höchstpersönliche Lebensbereich eines Menschen in einer Weise erörtert oder dargestellt, die geeignet ist, ihn in der Öffentlichkeit bloßzustellen, so hat der Betroffene gegen den Medieninhaber (Verleger) Anspruch auf eine Entschädigung für die erlittene Kränkung. Der Entschädigungsbetrag darf 20.000 Euro nicht übersteigen; im übrigen ist § 6 Abs. 1 zweiter Satz anzuwenden. […]

Urheberrechtsgesetz

§ 77. (1) **Briefe, Tagebücher und ähnliche vertrauliche Aufzeichnungen** dürfen weder öffentlich vorgelesen noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden, wenn dadurch berechtigte Interessen des Verfassers oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden. […]

§ 78. (1) **Bildnisse von Personen** dürfen weder öffentlich ausgestellt noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden, wenn dadurch berechtigte Interessen des Abgebildeten oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden. […]

§ 87. (2) Auch kann der Verletzte in einem solchen Fall eine angemessene Entschädigung für die in keinem Vermögensschaden bestehenden Nachteile verlangen, die er durch die Handlung erlitten hat. […] (inmaterieller Schadenersatz)

Ärztegesetz

§ 54. (1) Der Arzt und seine Hilfspersonen sind zur Verschwiegenheit über alle ihnen in Ausübung ihres Berufes anvertrauten oder bekannt gewordenen Geheimnisse verpflichtet. […]

Rechtsanwaltsordnung

§ 9. […] (2) Der Rechtsanwalt ist zur Verschwiegenheit über die ihm anvertrauten Angelegenheiten und die ihm sonst in seiner beruflichen Eigenschaft bekanntgewordenen Tatsachen, deren Geheimhaltung im Interesse seiner Partei gelegen ist, verpflichtet. Er hat in gerichtlichen und sonstigen behördlichen Verfahren nach Maßgabe der verfahrensrechtlichen Vorschriften das Recht auf diese Verschwiegenheit. […]

Beamten-Dienstrechtsgesetz

§ 46. (1) Der Beamte ist über alle ihm ausschließlich aus seiner amtlichen Tätigkeit bekanntgewordenen Tatsachen, deren Geheimhaltung im Interesse der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, der umfassenden Landesverteidigung, der auswärtigen Beziehungen, im wirtschaftlichen Interesse einer Körperschaft des öffentlichen Rechts, zur Vorbereitung einer Entscheidung oder im überwiegenden Interesse der Parteien geboten ist, gegenüber jedermann, dem er über solche Tatsachen nicht eine amtliche Mitteilung zu machen hat, zur Verschwiegenheit verpflichtet (Amtsverschwiegenheit). […]

StGB

Beharrliche Verfolgung

§ 107a. (1) Wer eine Person widerrechtlich beharrlich verfolgt (Abs. 2), ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.
(2) Beharrlich verfolgt eine Person, wer in einer Weise, die geeignet ist, sie in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt
1. ihre räumliche Nähe aufsucht,
2. im Wege einer Telekommunikation oder unter Verwendung eines sonstigen Kommunikationsmittels oder über Dritte Kontakt zu ihr herstellt,
3. unter Verwendung ihrer personenbezogenen Daten Waren oder Dienstleistungen für sie bestellt oder
4. unter Verwendung ihrer personenbezogenen Daten Dritte veranlasst, mit ihr Kontakt aufzunehmen.
(3) Hat die Tat den Selbstmord oder einen Selbstmordversuch der im Sinn des Abs. 2 verfolgten Person zu Folge, so ist der Täter mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems

§ 107c. (1) Wer im Wege einer Telekommunikation oder unter Verwendung eines Computersystems in einer Weise, die geeignet ist, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt
1. eine Person für eine größere Zahl von Menschen wahrnehmbar an der Ehre verletzt oder
2. Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung für eine größere Zahl von Menschen wahrnehmbar macht,
ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.
(2) Hat die Tat den Selbstmord oder einen Selbstmordversuch der im Sinn des Abs. 1 verletzten Person zu Folge, so ist der Täter mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Verletzung des Briefgeheimnisses und Unterdrückung von Briefen

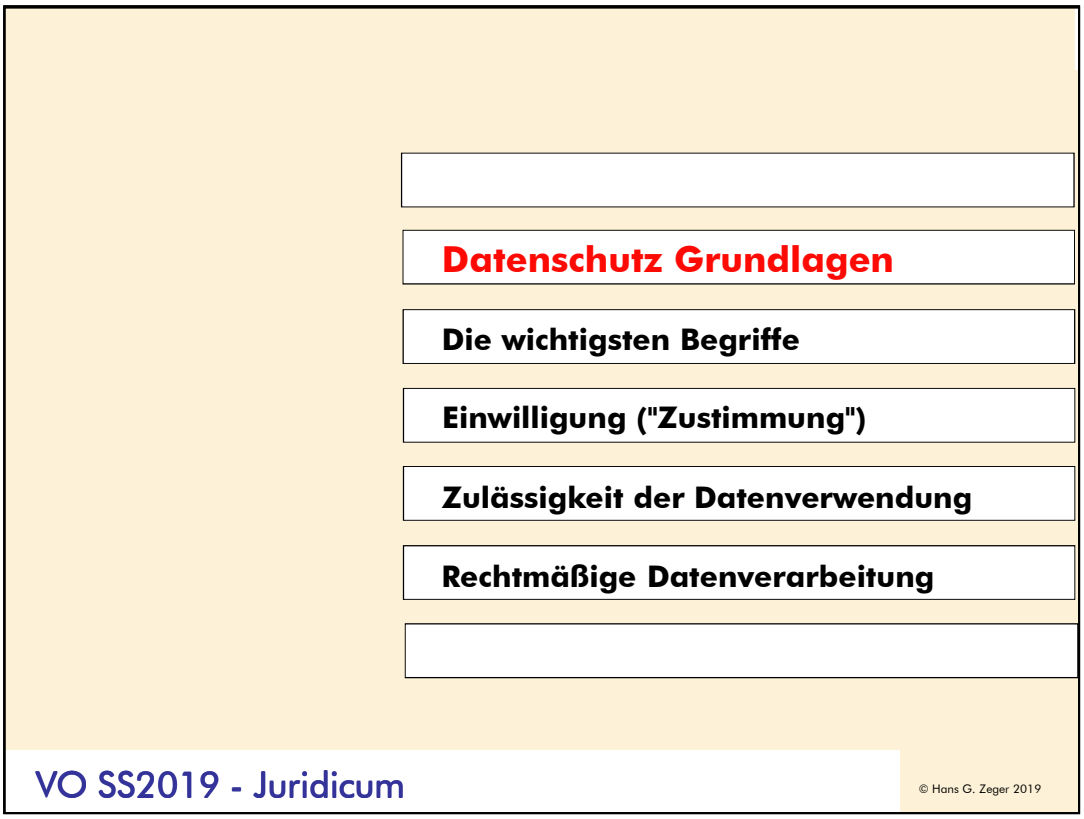
§ 118. (1) Wer einen nicht zu seiner Kenntnisnahme bestimmten verschlossenen Brief oder ein anderes solches Schriftstück öffnet, ist mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen.
(2) Ebenso ist zu bestrafen, wer, um sich oder einem anderen Unbefugten Kenntnis vom Inhalt eines nicht zu seiner Kenntnisnahme bestimmten Schriftstücks zu verschaffen,
1. ein verschlossenes Behältnis, in dem sich ein solches Schriftstück befindet, öffnet oder
2. ein technisches Mittel anwendet, um seinen Zweck ohne Öffnen des Verschlusses des Schriftstücks oder des Behältnisses (Z. 1) zu erreichen.
(3) Ebenso ist zu bestrafen, wer einen Brief oder ein anderes Schriftstück (Abs. 1) vor Kenntnisnahme durch den Empfänger unterschlägt oder sonst unterdrückt.
(4) Der Täter ist nur auf Verlangen des Verletzten zu verfolgen. Wird die Tat jedoch von einem Beamten in Ausübung seines Amtes oder unter Ausnützung der ihm durch seine Amtstätigkeit gebotenen Gelegenheit begangen, so hat die Staatsanwaltschaft den Täter mit Ermächtigung des Verletzten zu verfolgen.

Verletzung des Telekommunikationsgeheimnisses

§ 119. (1) Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Weitere StGB-Bestimmungen mit Konnex zu Privatsphäre und IT

§ 118a Widerrechtlicher Zugriff auf ein Computersystem
§ 119a Missbräuchliches Abfangen von Daten
§ 120 Mißbrauch von Tonaufnahme- oder Abhörgeräten
§ 121 Verletzung von Berufsgeheimnissen
§ 122 Verletzung eines Geschäfts- oder Betriebsgeheimnisses
§ 123 Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses
§ 124 Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands
§ 302 Mißbrauch der Amtsgewalt
§ 310 Verletzung des Amtsgeheimnisses


Datenschutz Grundlagen
Die wichtigsten Begriffe
Einwilligung ("Zustimmung")
Zulässigkeit der Datenverwendung
Rechtmäßige Datenverarbeitung
VO SS2019 - Juridicum
© Hans G. Zeger 2019

-

DSGVO - Grundlagen

Entwicklung Datenschutz in Österreich

1978 erstes Datenschutzgesetz - DSG (BGBl. Nr. 565/1978)
(Geltung 1.1.1980-31.12.1999)
1995 EG-Datenschutzrichtlinie 95/46/EG
1999 Datenschutzgesetz - DSG 2000 (BGBl. I Nr. 165/1999)
(Geltung 1.1.2000-24.5.2018)
2016 DSGVO (EU) 2016/679
2017 DSG Anpassungsgesetz (DSAG 2018)
2018 DSG Deregulierungsgesetz
2018 Anwendung der DSGVO
(Geltung ab 25.5.2018)

Was kommt noch auf uns zu?

✓ 5/2018 Verordnung Liste Verarbeitungen mit "ohne" Risiko
✓ 11/2018 Verordnung Liste Verarbeitungen mit hohem Risiko
??/20?? AT-Regelung wann verpflichtende Konsultation der DSB erforderlich ist
??/20?? Akkreditierung von Datenschutz-Zertifizierungsstellen
??/20?? EU-weite Durchführungsbestimmungen und Rechtsakte der EU-Kommission

VO SS2019 - Juridicum

Entwicklung des Datenschutzes in Österreich

Eine Übersicht findet sich unter
http://www.argedaten.at/php/cms_monitor.php?q=PUB&s=13498rlh

Änderungen zum DSG 2000 (historisch)

2001 Euro-Umstellung der Verwaltungsstrafen (BGBl. I Nr. 136/2001)

2005 "Tsunami"-Bestimmung (BGBl. I Nr. 13/2005)

2008 Änderungen in Verfassungsbestimmungen (BGBl. I Nr. 2/2008)

2009 DSG 2000 - Novelle 2010 (BGBl. I Nr. 133/2009)
u.a. Regelung der Videoüberwachung

2012 Verwaltungsgerichtsbarkeits-Novelle 2012 (BGBl. I Nr. 51/2012)
Abschaffung der Datenschutzkommission, Überführung der Agenden der Kommission in den Bundesverwaltungsgerichtshof

2013 DSG 2000 - Novelle 2013 (BGBl. I Nr. 57/2013)
Anpassung der Datenschutzkommission an die Unabhängigkeitsanforderungen nach dem EUGH-Urteil

2013 DSG 2000 - Novelle 2014 (BGBl. I Nr. 83/2013)
Regelung der Kompetenzen der Datenschutzbehörde (1. Instanz) und der Datenschutzagenden des Bundesverwaltungsgerichtshofs (2. Instanz)

2013 Novelle der Datenschutzangemessenheits-Verordnung (BGBl. II Nr. 150/2013 - DSAV-Novelle 2013)

2013 Datenschutzanpassungs-Verordnung 2013 (BGBl. II Nr. 213/2013)

EU Datenschutz-Grundverordnung

http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679

EU-Neuregelung des Datenschutzes

Fahrplan zur EU DSGVO

- 4.11.2010 Kommissionsmitteilung Konzept für neues Datenschutzrecht zu entwickeln
- bis 14.1.2011 europaweites Konsultationsverfahren
- 25.1.2012 Entwurf einer EU-Grundverordnung Datenschutz
- 21.10.2013 Abstimmung im LIBE-Ausschuß des EU-Parlaments (Verhandlungsmandat des Parlaments)
- 15.6.2015 Rats-Arbeitsgruppe beschließt gemeinsame Position
- 17.12.2015 abstimmungsfähiger Endentwurf
- 14.4.2016 Beschluss Europäisches Parlament
- 2017/2018 Nationale Durchführungsgesetze erforderlich
- 25.5.2018 Geltung der EU-Grundverordnung Datenschutz (DSGVO) EU-weit + DSG in Österreich

VO SS2019 - Juridicum

Informationen zur weiteren Entwicklung der EU-Verordnung:

https://www.argedaten.at/php/cms_monitor.php?q=PUB&s=63852ono

EU-Neuregelung des Datenschutzes

Was ist die Datenschutz-Grundverordnung?

- unmittelbar wirksam: Betriebe, Behörden, Gerichte MÜSSEN die Bestimmung direkt anwenden
- bisher: die Datenschutzrichtlinie wurde von den Parlamenten der 28 Mitgliedsstaaten teilweise nach Gutdünken interpretiert und umgesetzt, das Berufen direkt auf die Richtlinie war nur schwierig und über Umwege möglich
- die DSGVO ist ein Kompromiss der Mitgliedsstaaten, bei dem sich der Rat gegenüber der Kommission wesentlich durchgesetzt hat
- auf Grund des Kompromisses gibt es etwa 27 Verweise auf nationale Bestimmungen und Gestaltungsmöglichkeiten (fälschlich "Öffnungsklauseln" genannt)
- abhängig vom "Mut" der EU-Staaten werden nationale Gestaltungsspielräume wieder zu unterschiedlicher Handhabung des Datenschutzes in der EU führen
- der Gefahr des Abdriftens in nationale Befindlichkeiten stehen das "Koheränzverfahren" und der EU-Datenschutzausschuss gegenüber

VO SS2019 - Juridicum

-

DSGVO Grundlagen

Eckpfeiler der neuen DSGVO

- Dokumentation und Folgenabschätzung (Art. 30, 35, 36)
  - ✓ detailliertes Verzeichnis der Verarbeitungstätigkeiten ist zu führen
  - ✓ Risken einer Verarbeitung sind zu bewerten (zB Profiling, automatisierte Entscheidungen, Übermittlungen)
  - ✓ Pflicht zur Vorabkonsultation der Aufsichtsbehörde bei "hohem" Risiko
- verpflichtender Datenschutzbeauftragter (Art. 37)
  - ✓ alle öffentlichen Einrichtungen
  - ✓ Kerntätigkeit erfordert umfangreiche regelmäßige und systematische Beobachtung der Betroffenen
  - ✓ Kerntätigkeit ist die umfangreiche Verarbeitung besonderer Kategorien von Daten
  - ✓ Kerntätigkeit ist die umfangreiche Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten

VO SS2019 - Juridicum

-

Eckpfeiler der neuen DSGVO II

- abgestufte Geldbußen (Art. 83)
  - ✓ bis 10 Mio Euro (bei Unternehmen bis 2% Umsatz), ua bei Verletzung von Aufzeichnungspflichten
  - ✓ bis 20 Mio Euro (bis 4% Umsatz), ua bei Verletzung von Betroffenenrechten
  - ✓ Verantwortlich ist die Aufsichtsbehörde
  - ✓ keine Mindeststrafen vorgesehen
- neue Begriffe (Art. 4)
  - ✓ "Profiling": Bewertung von Personen
  - ✓ "Pseudonymisierung": technische oder rechtliche Trennung von Personendaten und Identifikationsdaten
  - ✓ "Hauptniederlassung": Stelle an der Verarbeitungsentscheidungen getroffen werden
  - ✓ "Unternehmensgruppe": Gruppe von Unternehmen, die von einem Unternehmen abhängig sind
- neue "besondere Kategorien" von Daten (Art. 9)
  - ✓ genetische Daten, biometrische Daten

-

Eckpfeiler der neuen DSGVO III

- "doppeltes" One-Stop-Shop-System:
  a) je Verantwortlichen/Auftragsverarbeiter ist nur eine Aufsichtsstelle zuständig
  (Hauptniederlassung des Verantwortlichen/Auftragsverarbeiters, statt bisher für jede Niederlassung die jeweilige nationale Behörde)
  b) jeder Betroffene kann sich bei Beschwerden gegen alle Verantwortliche gemäß DSGVO an seine nationale Aufsichtsbehörde wenden
- Einführung neuer "Prinzipien":
  ✓ Recht auf "Vergessenwerden": Löschen + Verständigungspflicht (Art. 17 + 19)
  ✓ Förderung technischer Datenschutzmaßnahmen ("data protection by design") (EW 61)
  ✓ Privatsphäreeinstellungen sollen Standard werden ("data protection by default") (EW 61)

-

Datenschutz-Anpassungsgesetz(e)

DSG

- 5 Hauptstücke
- formal: Änderung des DSG 2000
- Verfassungsbestimmungen des DSG 2000 bleiben auf Grund parteipolitischer Patt-Situation unverändert
- §1 DSG 2000 steht im offensichtlichen Widerspruch zur DSGVO
- Verzicht auf eigene Begriffsbestimmungen

Hauptstück 1: DSGVO Anpassungen	✓ **wird behandelt**
Hauptstück 2: Organe	✓ **DSB wird behandelt**
Hauptstück 3: Umsetzung DS-Richtlinie Sicherheitsbehörden	✗ **nicht behandelt**
Hauptstück 4: Strafbestimmungen	✓ **wird behandelt**
Hauptstück 5: Schlussbestimmungen	✓ **wird behandelt**

VO SS2019 - Juridicum

-

DSGVO - Grundlagen

EU-Verordnung DSGVO (2016)

"Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG"

Art. 1 Abs. 1 "Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten."

Art. 1 Abs. 2 "Schutz der Grundrechte und Grundfreiheiten und insbesondere deren Recht auf Schutz personenbezogener Daten."

Art. 1 Abs. 3 "Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden"

DSGVO gilt nur für "natürliche Personen"
ab 5/2018 KEINE Datenschutzrechte (iS der **DSGVO**) für "juristische und sonstige Personen")

Bestimmungen betreffen alle Verwendungsformen persönlicher Daten, nicht nur automatisiert verarbeitete Daten (Art. 2 Abs. 1)

VO SS2019 - Juridicum

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Die Richtlinie soll gleichermaßen den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten sichern

DSGVO Art. 1 Gegenstand und Ziele

(1)Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2)Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(3)Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

DSGVO - Grundlagen

DSGVO "Anwendung"

Grundsätzlich gilt die DSGVO für alle Verwendungen personenbezogener Daten "für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen" (EW26), insbesondere auch für folgende Bereiche:

- **EW153**: journalistische Tätigkeit
- **EW158**: Archivzwecke
- **EW159**: wissenschaftliche Forschungszwecke
- **EW160**: historische Forschung
- **EW161**: klinische Forschung
- **EW162**: statistische Zwecke
- **EW165**: religiöse Angelegenheiten

Jedoch Erleichterungen und Abweichungen, auf Grund nationaler Gesetze, bestehender völkerrechtlicher Vereinbarungen oder anderer EU-Bestimmungen

VO SS2019 - Juridicum

DSGVO EW153

Im Recht der Mitgliedstaaten sollten die Vorschriften über die freie Meinungsäußerung und Informationsfreiheit, auch von Journalisten, Wissenschaftlern, Künstlern und/oder Schriftstellern, mit dem Recht auf Schutz der personenbezogenen Daten gemäß dieser Verordnung in Einklang gebracht werden. Für die Verarbeitung personenbezogener Daten ausschließlich zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken sollten Abweichungen und Ausnahmen von bestimmten Vorschriften dieser Verordnung gelten, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit dem Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit, wie es in Artikel 11 der Charta garantiert ist, in Einklang zu bringen. Dies sollte insbesondere für die Verarbeitung personenbezogener Daten im audiovisuellen Bereich sowie in Nachrichten- und Pressearchiven gelten. Die Mitgliedstaaten sollten daher Gesetzgebungsmaßnahmen zur Regelung der Abweichungen und Ausnahmen erlassen, die zum Zwecke der Abwägung zwischen diesen Grundrechten notwendig sind. Die Mitgliedstaaten sollten solche Abweichungen und Ausnahmen in Bezug auf die allgemeinen Grundsätze, die Rechte der betroffenen Person, den Verantwortlichen und den Auftragsverarbeiter, die Übermittlung von personenbezogenen Daten an Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden, die Zusammenarbeit und Kohärenz und besondere Datenverarbeitungssituationen erlassen. Sollten diese Abweichungen oder Ausnahmen von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein, sollte das Recht des Mitgliedstaats angewendet werden, dem der Verantwortliche unterliegt. Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, weit ausgelegt werden.

DSGVO - Grundlagen

DSGVO Art. 2 Abs. 2 "Keine Anwendung"

- Tätigkeiten die nicht in den Anwendungsbereich des Unionsrechts fallen (zB Internationale Organisationen)
- Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten
- unstrukturierte Informationssammlungen ohne Automationsunterstützung (Akteninhalte, "Zettelwirtschaft")
- Behördentätigkeit im Rahmen der Strafverfolgung, der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (⇨ **eigene Datenschutzrichtlinie**)

weiters keine Anwendung:

- Verstorbene (EW27, EW160)

VO SS2019 - Juridicum

DSGVO Art. 2 Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,

c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,

d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

DSGVO EW27

Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.

DSGVO EW160

Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu historischen Forschungszwecken gelten. Dazu sollte auch historische Forschung und Forschung im Bereich der Genealogie zählen, wobei darauf hinzuweisen ist, dass diese Verordnung nicht für verstorbene Personen gelten sollte.

DSGVO - Grundlagen

DSGVO Art. 3 Abs 2 "räumliche Anwendung"

- bei Tätigkeiten im Rahmen einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet
- auf alle sonstigen Verantwortlichen oder Auftragsverarbeiter, bei
  a) Angebot von Waren und Dienstleistungen an in der EU befindliche Bürger (unabhängig ob gegen Bezahlung oder gratis)
  b) Beobachtung von Verhalten von ***Personen***, soweit es innerhalb der EU stattfindet
- alle Verantwortlichen (unabhängig vom Sitz) soweit er dem Recht eines Mitgliedsstaates unterliegt

VO SS2019 - Juridicum

DSGVO Art. 3 Räumlicher Anwendungsbereich

(2)Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

DSGVO - Grundlagen

DSGVO Art 4 Z 1 "personenbezogene Daten"

"alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen"

DSGVO Art. 4 Z 2 "Verarbeitung"

"jeden Vorgang oder Vorgangsreihe wie das Erheben, das Erfassen, 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"

VO SS2019 - Juridicum

DSGVO Art. 4 Begriffsbestimmungen

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, 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;

DSGVO - Grundlagen

DSGVO Art. 4 Z 7 "Verantwortlicher"

"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"

DSGVO Art. 4 Z 8 "Auftragsverarbeiter"

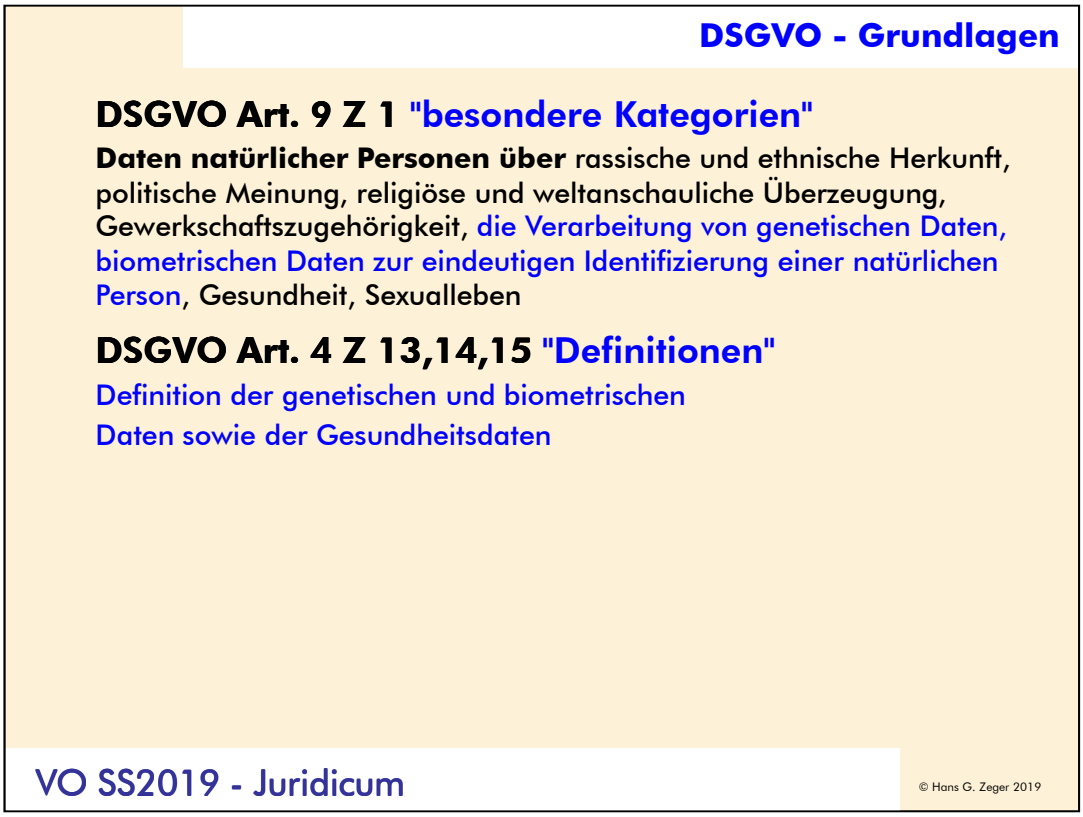
natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

VO SS2019 - Juridicum

DSGVO Art. 4 Begriffsbestimmungen

7. „Verantwortlicher“ die 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

8.„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;



DSGVO Art. 9 Abs. 1 Verarbeitung besonderer Kategorien personenbezogener Daten

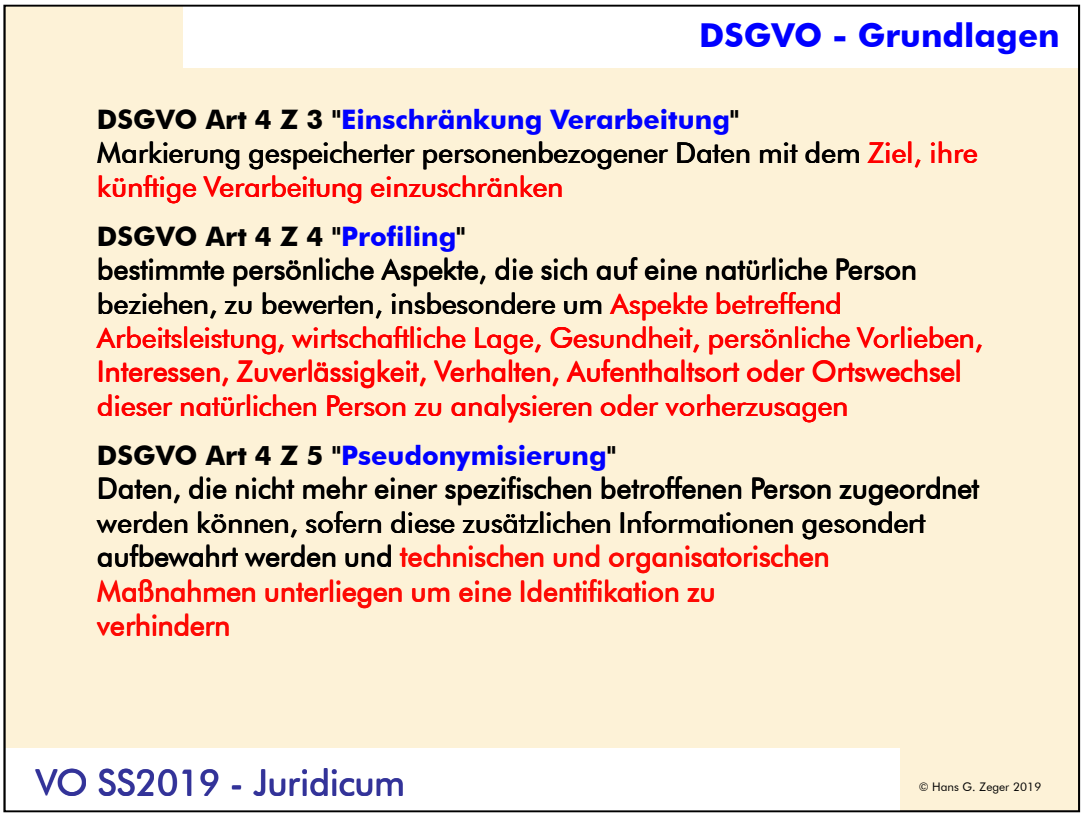
(1)Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

DSGVO Art. 4 Begriffsbestimmungen

13. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

14. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

15. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

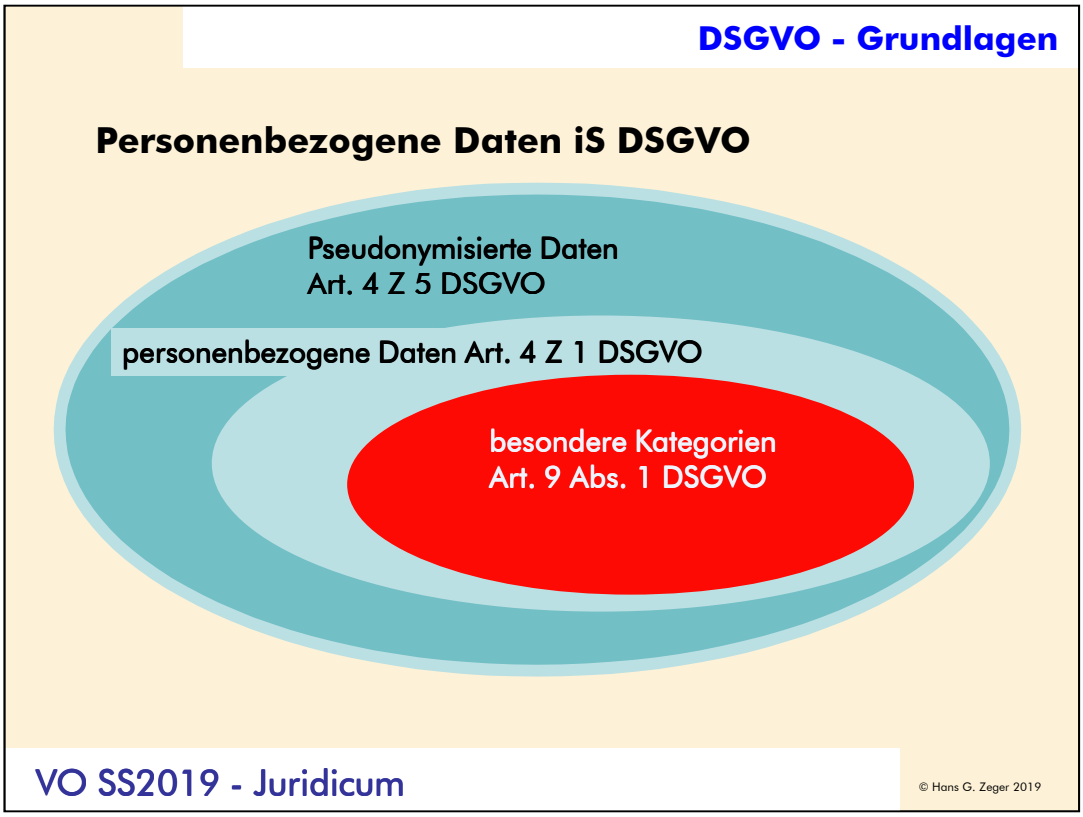


DSGVO Art. 4 Begriffsbestimmungen

3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;


DSGVO - Grundlagen
Personenbezogene Daten iS DSGVO
Pseudonymisierte Daten
Art. 4 Z 5 DSGVO
personenbezogene Daten Art. 4 Z 1 DSGVO
besondere Kategorien
Art. 9 Abs. 1 DSGVO
VO SS2019 - Juridicum
© Hans G. Zeger 2019

-

DSGVO - Grundlagen

DSGVO Art. 4 Z 11 "Einwilligung"

"jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist"
(weitere Details und Widerruf der Einwilligung in Art. 7 geregelt)

Von Einwilligung/Zustimmung sind andere rechtlich zulässige Nutzungen von Daten zu unterscheiden, etwa im Rahmen von Bestellungen, Kundenkarten, ...

VO SS2019 - Juridicum

DSGVO Art. 4 Begriffsbestimmungen

11.„Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

DSGVO - Grundlagen

DSGVO Art 4 Z 16 "Hauptniederlassung"
Verantwortlicher mit Niederlassungen in mehreren EU-Staaten, kann jene zur Hauptniederlassung erklären, an der die Entscheidungen getroffen werden ⇨ Zuständigkeit der Aufsichtsbehörde (Art. 51ff)

DSGVO Art 4 Z 18 "Unternehmen"
natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform

DSGVO Art 4 Z 19 "Unternehmensgruppe"
Gruppe, die aus herrschenden Unternehmen und den von diesem herrschenden Unternehmen abhängigen Unternehmen ⇨ Datenschutzbeauftragten (Art. 37), Unternehmensvorschriften (Art. 47), Beschäftigtendaten (Art. 88)

Keine Konzernerleichterung, aber: "Wird die Verarbeitung durch eine Unternehmensgruppe vorgenommen, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten, es sei denn, die Zwecke und Mittel der Verarbeitung werden von einem anderen Unternehmen festgelegt." (EW 38)

VO SS2019 - Juridicum

DSGVO Art. 4 Begriffsbestimmungen

16. „Hauptniederlassung“

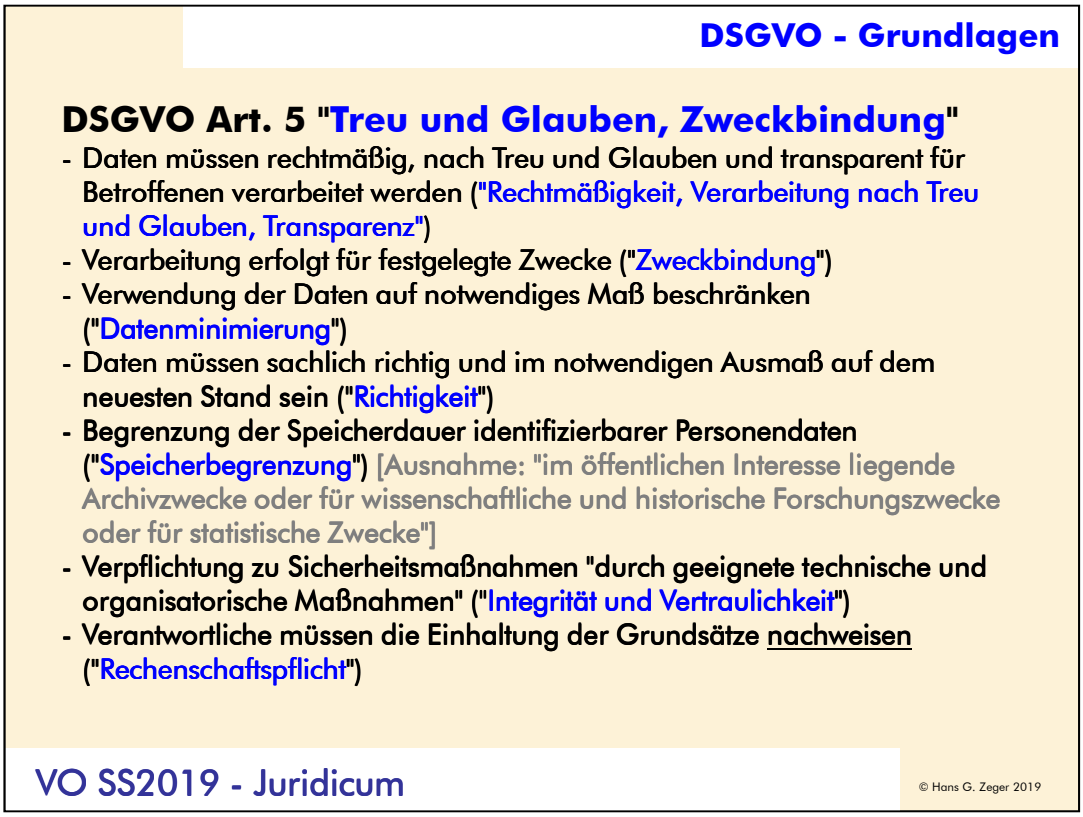
a) im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;

b) im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;

17. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

18. „Unternehmen“ eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

19. „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;



DSGVO Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

(1)Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

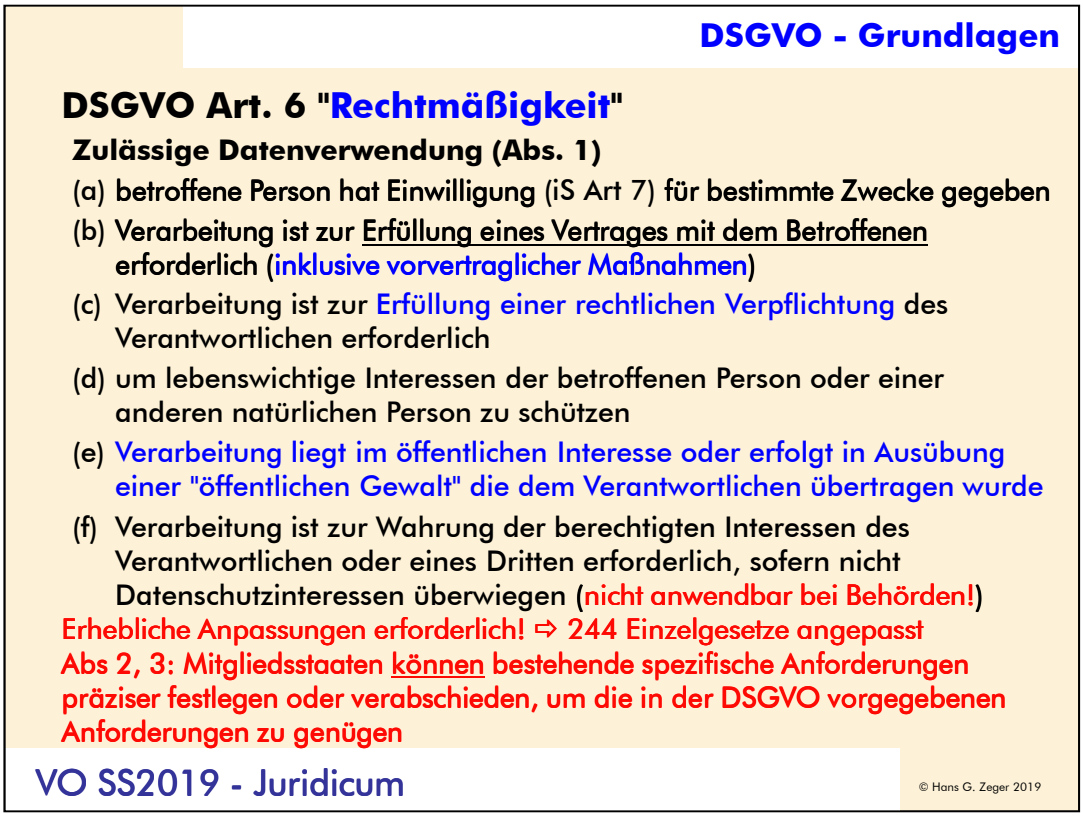
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2)Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).



DSGVO Art. 6 Rechtmäßigkeit der Verarbeitung

(1)Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

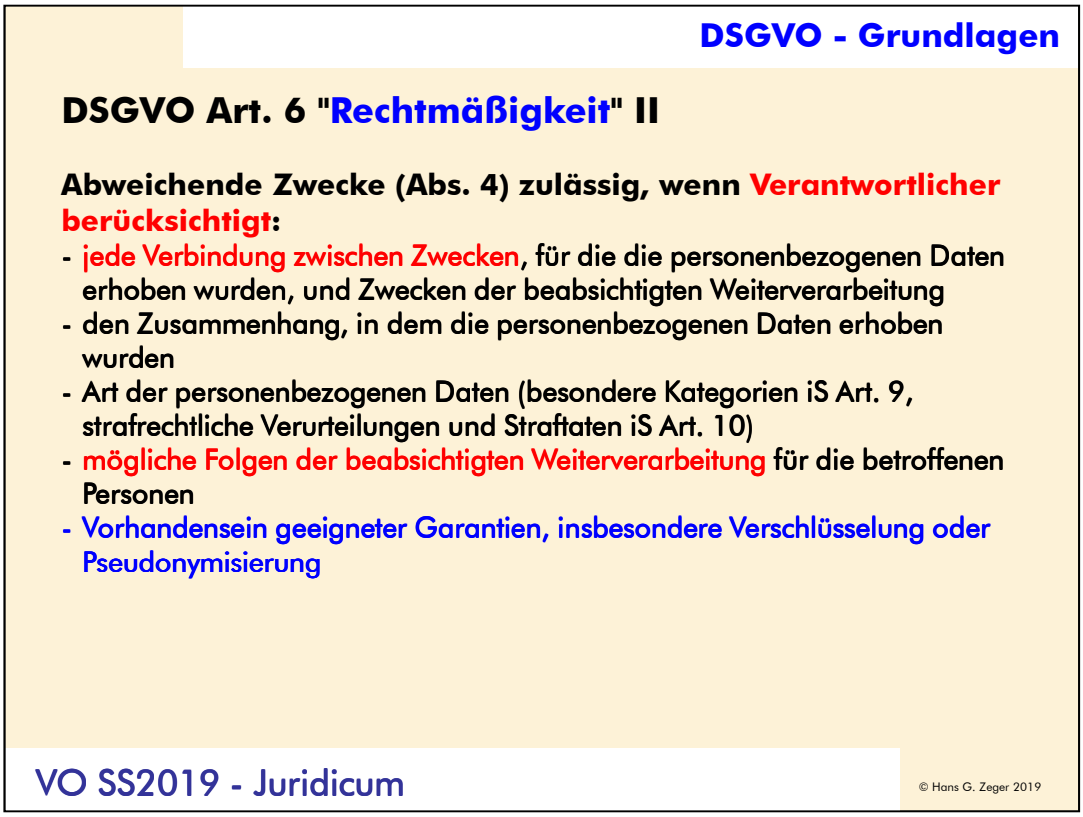
Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2)Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3)Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.



DSGVO Art. 6 Rechtmäßigkeit der Verarbeitung (Fortsetzung)

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4)Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche — um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist — unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen, e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

DSGVO - Grundlagen

DSGVO Art. 9 "besondere Datenkategorien"

Grundsätzliches Verarbeitungsverbot (Abs. 1)

- rassischer und ethnischer Herkunft
- politische Meinung
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- genetischen Daten
- biometrischen Daten zur eindeutigen Identifizierung
- Gesundheit
- Sexualleben oder sexuellen Orientierung

Ausnahmen vom Verarbeitungsverbot (Abs. 2)

(a) Einwilligung durch Betroffenen, jedoch Einwilligung kann auch verboten werden [Anm: AT siehe Gentechnikgesetz]

(b) Verarbeitung aus Gründen sozialer Sicherheit und Sozialschutzes erforderlich

(c) lebenswichtige Interessen erfordern Verwendung und Betroffener ist außerstande eine Einwilligung zu geben

VO SS2019 - Juridicum

DSGVO Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten

(1)Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2)Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,

c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,

d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

DSGVO Art. 9 "besondere Datenkategorien" II

Ausnahmen vom Verarbeitungsverbot (Abs. 2) Fortsetzung

(d) Verarbeitung erfolgt durch Organisation im Rahmen ihrer Tätigkeit (gilt ausschließlich für Organisation ohne Gewinnerzielungsabsicht und nur für ihre Mitglieder bzw. ehemaligen Mitglieder

(e) Daten wurden vom Betroffenen offensichtlich öffentlich gemacht

(f) Verarbeitung dient zur Geltendmachung von Rechtsansprüchen oder im Rahmen gerichtlicher Handlungen

(g) Unionsrecht oder nationales Recht sieht Verarbeitung vor, bei Wahrung des Rechts auf Datenschutz [Anm: ELGA-Gesetz?]

(h) Verarbeitung zum "*Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich*" erforderlich

DSGVO Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten (Fortsetzung)

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

DSGVO Art. 9 "besondere Datenkategorien" III

Ausnahmen vom Verarbeitungsverbot (Abs. 2) Fortsetzung

(i) Verarbeitung aus "*Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten*" erforderlich

(j) Verarbeitung ist für in "*öffentlichem Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke*" erforderlich

Sonstige Verarbeitungsbeschränkungen (Abs. 3, 4)

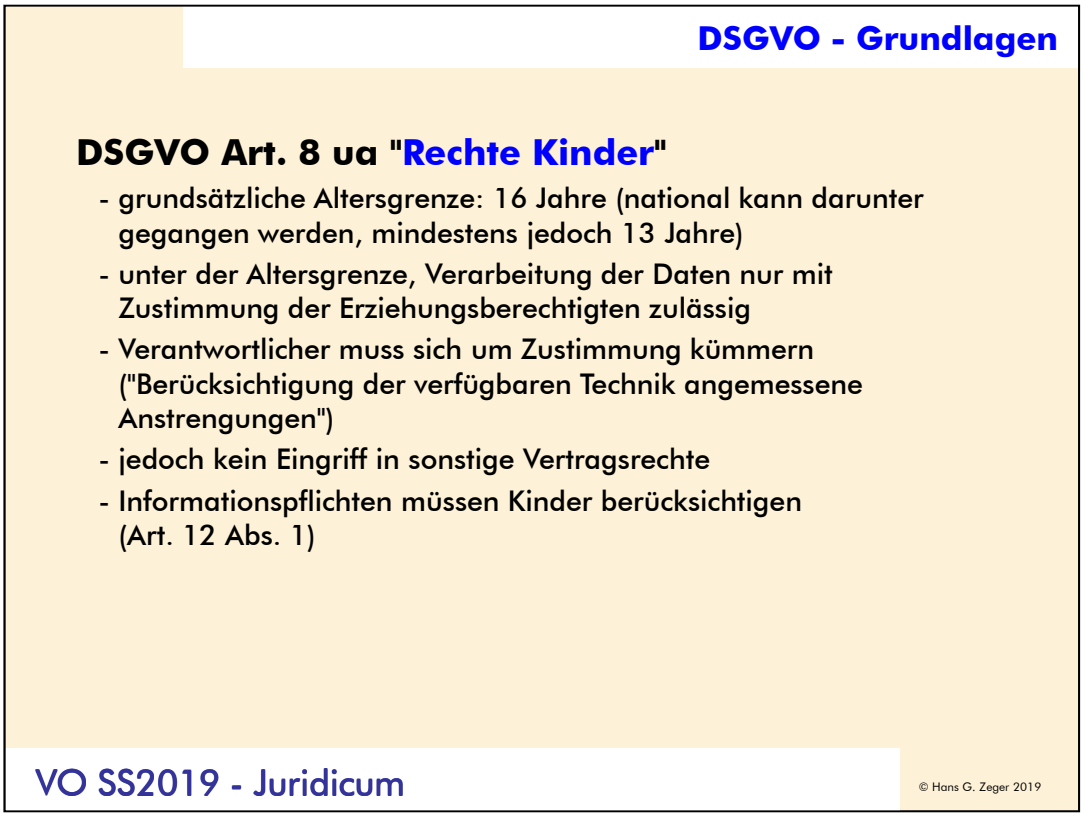
- im Rahmen der Gesundheitsvorsorge/-versorgung (iS Abs. 2 lit h): erfordert Fachpersonal, das einem Berufsgeheimnis unterliegt bzw. Personen unter dessen Verantwortung (ebenfalls Geheimhaltungspflicht erforderlich)
- Mitgliedsstaaten können zusätzliche Bedingungen inklusive Beschränkungen einführen (bzw. aufrecht erhalten) die genetische, biometrische oder Gesundheitsdaten betreffen

DSGVO Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten (Fortsetzung)

j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

(3)Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4)Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.



DSGVO Art. 8 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

(1)Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.

Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.

(2)Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.

(3)Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.

DSGVO Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1)Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

DSGVO Art. 26 "Gemeinsame Verarbeitung"

- gemeinsame Verarbeitung zulässig
- muss transparent vereinbart sein
- Verteilung der Aufgaben und Pflichten muss eindeutig geregelt sein
- Betroffene können ihre Rechte gegenüber jedem einzelnen Verantwortlichen wahrnehmen

DSGVO Art. 26 Gemeinsam für die Verarbeitung Verantwortliche

(1)Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2)Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3)Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

DSGVO - Grundlagen

Wie kann die Rechtmäßigkeit einer Datenverarbeitung abgeschätzt werden?

(1) Rechtsgrundlage
Die Verwendung von personenbezogenen Daten muss für ein legitimes Ziel (Gesetz, Vertrag, ...) erforderlich sein.

(2) Eignung
Die Verwendung von Daten muss geeignet sein um das bestimmte, konkrete Ziel (Zweck) tatsächlich zu erreichen.

(3) Erforderlichkeit
Es gibt keine alternative (weniger invasive) Lösung zur Erreichung des bestimmten Ziels (Zweckes).

(4) Verhältnismäßigkeit
Die Verwendung der Daten führt zu keiner Verletzung höherwertiger Schutzrechte (Grundrechte).

VO SS2019 - Juridicum

-

DSGVO - zuständige Stellen

Einrichtungen / Zuständigkeiten zum Datenschutz

- **Datenschutzbehörde *(formlos)***
  - Beschwerdestelle für Betroffene in allen Fällen
  - Aufsichtsstelle für alle Verantwortliche und Auftragsverarbeiter, die ihre Hauptniederlassung in AT haben
  - Strafbehörde bei Datenschutzverletzungen nach DSGVO und DSG
  - Kontroll-, Beratungs- und Informationsbefugnisse
  - Ansprechstelle in EU-Koheränzverfahren
- **Bundesverwaltungsgericht *(formlos)***
  - Beschwerdeinstanz gegen Entscheidungen der Datenschutzbehörde
- **Zivilgericht *(Anwaltspflicht)***
  - bei Schadenersatzklagen
  - *alle Datenschutzfragen (strittig)*
- **Staatsanwaltschaft / Polizei *(formlos)***
  Anzeigen gem. § 63 DSG

VO SS2019 - Juridicum

Zivilgerichte - 16 Landesgerichte zuständig:

LG Eisenstadt, Feldkirch, Zivilrechtssachen Graz, Innsbruck, Klagenfurt, Korneuburg, Krems a/d Donau, Leoben, Linz, Ried/Innkreis, Salzburg, St. Pölten, Steyr, Wels, Zivilrechtssachen Wien, Wr. Neustadt

(http://www.bmj.gv.at/_cms_upload/_docs/gerichte_und_behoerden2005.pdf)

Internet und Datenschutz

In welchem Umfang sind DSG/DSGVO auf das Internet anwendbar?
Dazu sind Vorfragen zu klären:

- Ist eine Veröffentlichung auf einer Internetseite eine Datenverarbeitung?
- Ist eMail-Verkehr eine Datenverarbeitung?
- Wann handelt es sich um personenbezogene Daten?
  Was sind die Mindestangaben, um von Personenbezug sprechen zu können?
  Name, Adresse, Identifikationsdaten
  eMail-Adresse
  IP-Adresse, Matrikelnummer (z.B. e0640132)
  Kundennummer/Benutzerkennung
  Cookies, Computersignatur, ...
- Ist ein berechtigter Zweck gegeben?

VO SS2019 - Juridicum

-

Beispiele / Entscheidungen

- Webseite als Datenverarbeitung
- Bedeutung der IP-Adresse
- Veröffentlichung von Informationen
- Web-Zugriffsstatistik
- Zweck der Datenverarbeitung

VO SS2019 - Juridicum

-

Beispiele / Entscheidungen

EuGH-Entscheidung C-101/01 Fall Lindqvist

Frau Lindqvist war/ist Reinigungskraft
besuchte einen Web-Programmierkurs
ehrenamtlich in der lokalen Kirche tätig

Produzierte eine persönliche Webseite
enthalten:

- Informationen über sich und Ehemann
- 16 namentlich genannte Konfirmanten/Kirchenmitarbeiter
- "lustige" Beschreibung der Interessen dieser Personen
- Information über eine Beinverletzung einer Person und dass sie nicht am Unterricht teilnehmen kann

VO SS2019 - Juridicum

-

Beispiele / Entscheidungen

EuGH-Entscheidung C-101/01 Lindqvist II

Frau Lindqvist löscht sofort nach Verlangen

- trotzdem Strafverfahren, weil Datenverarbeitung nicht registriert
- Strafe von 4000 SEKronen (ca. 430 Euro)

Im Zuge des Verfahrens wurde EuGH von schwedischem Gericht mit einer Reihe von Fragen angerufen:

- Ist eine Website eine Datenverarbeitung? JA
- Gelten die Ausnahmebestimmungen für private Webseiten? NEIN
- Handelt es sich um sensitive Daten? JA
- Liegt (genehmigungspflichtiger) internationaler Datenverkehr vor? NEIN
- Schränkt das EG-Datenschutzrecht unzulässig die Freiheit der Meinungsäußerung ein? NEIN
- Gibt die Richtlinie 95/46/EG nur einen Mindeststandard vor? NEIN

DSGVO ⇨ Entscheidung vergleichbar

VO SS2019 - Juridicum

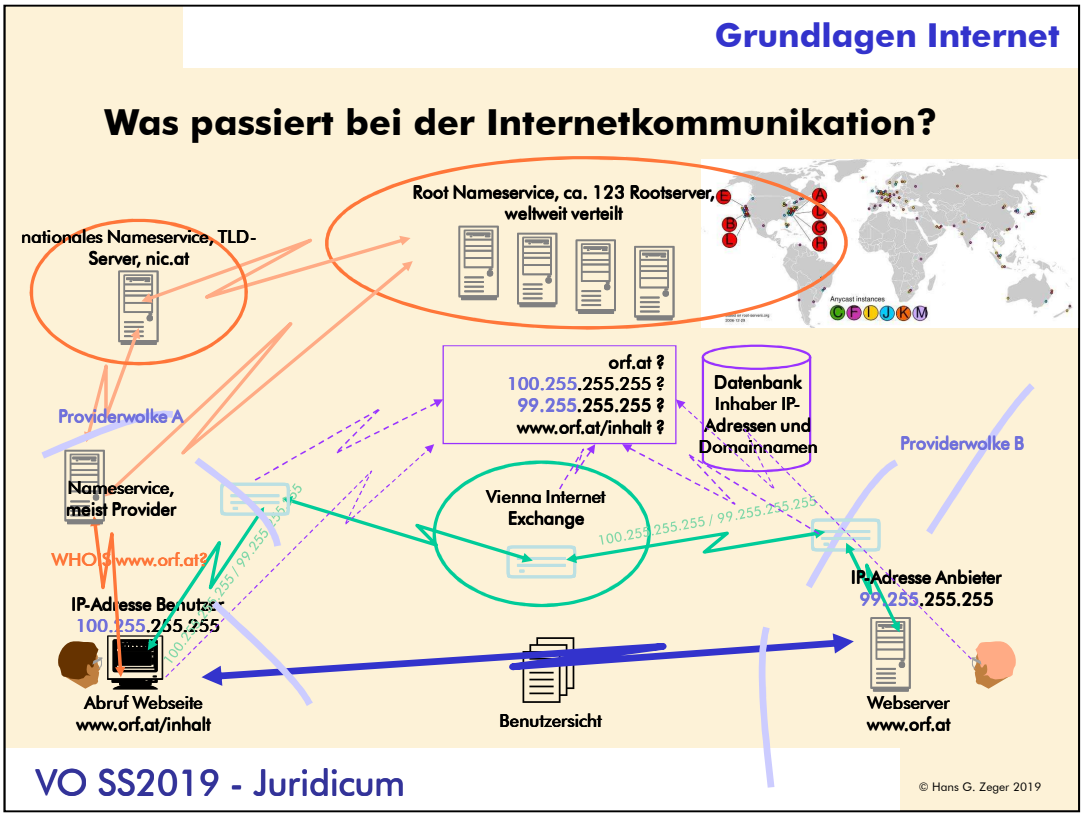
Ausnahme des Art. 3 Abs. 2 95/46/EG (Anwendungsbereich):

...

(2) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,

...

– die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.


Grundlagen Internet
Was passiert bei der Internetkommunikation?
Root Nameservice, ca. 123 Rootserver, weltweit verteilt
nationales Nameservice, TLD-Server, nic.at
orf.at ?
100.255.255.255 ?
99.255.255.255 ?
www.orf.at/inhalt ?
Datenbank Inhaber IP-Adressen und Domainnamen
Providerwolke A
Providerwolke B
Nameservice, meist Provider
Vienna Internet Exchange
WHOIS www.orf.at?
IP-Adresse Benutzer
100.255.255.255
IP-Adresse Anbieter
99.255.255.255
Abruf Webseite www.orf.at/inhalt
Benutzersicht
Webserver www.orf.at
VO SS2019 - Juridicum
© Hans G. Zeger 2019

-

Grundlagen Internet

Wie erfahre ich etwas über Internetkommunikation?

- IP-Adress(Range)-Information (http://www.db.ripe.net/)
- IP-Lookup-Information (http://www.dnsstuff.com/)
- Traceroute (http://www.dnsstuff.com/)
- Domain-Name-Service (http://www.dnsstuff.com/)
- Standortinformation (http://www.ip-adress.com/)
- System-Information zu eMail, Browser, Server (http://www.netcraft.com)
- Portscan/Schwachstellenanalyse (http://www.nessus.org/)

Beispiele IP-Adressen:

- 194.232.104.22 [ORF]
- 91.114.3.197 [Erste Sparinvest]
- 91.112.60.226, 91.112.191.38, 88.117.177.94 [persönliche Adressen]
- 92.193.83.188, 88.117.118.76 [Dynamic IP Addresses]

VO SS2019 - Juridicum

-

Beispiele / Entscheidungen

Ist IP-Adresse eine personenbezogene Information?

(BGH VI ZR 135/13 / EuGH-Urteil 2016/10/19 Breyer C-582/14**)**

Frage 1 (gekürzt): Ist eine IP-Adresse, die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum, wenn ein Dritter (hier: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?

EuGH: "... [ist für] **Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen"**

Konsequenz: Die Beurteilung ob eine bestimmte Information personenbezogen ist oder nicht, hängt nicht nur von den dem Verantwortlichen verfügbaren Möglichkeiten der Bestimmung der Person ab, sondern auch welche (rechtliche) Möglichkeiten er hat Zusatzinformationen Dritter zu nutzen

VO SS2019 - Juridicum

Dem Gerichtshof der Europäischen Union werden gemäß Art.267 AEUV folgende Fragen zur Auslegung des Unionsrechts vorgelegt:

1. Ist Art.2 Buchstabe a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verar-beitung personenbezogener Daten und zum freien Datenverkehr (Abl. EG 1995, L 281/31) Datenschutz-Richtlinie - dahin auszulegen, dass eine Internetprotokoll-Adresse (IP-Adresse), die ein Diensteanbieter im Zusammenhang mit einem Zu-griff auf seine Internetseite speichert, für diesen schon dann ein personenbezoge-nes Datum darstellt, wenn ein Dritter (hier: Zugangsanbieter) über das zur Identifi-zierung der betroffenen Person erforderliche Zusatzwissen verfügt?

2. Steht Art.7 Buchstabe f der Datenschutz-Richtlinie einer Vorschrift des nationalen Rechts entgegen, wonach der Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden darf, soweit dies erforderlich ist, um die konkrete Inanspruchnahme des Telemediums durch den jeweiligen Nutzer zu ermöglichen und abzurechnen, und wonach der Zweck, die generelle Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung nicht über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann?

BGH, Beschluss vom 28. Oktober 2014 - VI ZR 135/13 - LG Berlin, AG Berlin-Mitte

EuGH-URL: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62014CJ0582

ad Frage 1. Art. 2 Buchst. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass eine dynamische Internetprotokoll-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den **Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen**.

Beispiele / Entscheidungen

Ist IP-Adresse eine personenbezogene Information? II

(BGH VI ZR 135/13 / EuGH 2016/10/19 Breyer C-582/14**)**

Frage 2 betrifft: Umfang der im Rahmen eines Online-Dienstes zulässigerweise gespeicherten Daten

EuGH: Umfang ist in Richtlinie 95/46/EG abschließend geregelt, insbesondere Art. 7 lit f darf durch innerstaatliche Regelungen weder eingeschränkt, noch erweitert werden

Konsequenz: Im konkreten Fall war die Frage zu klären, ob die Bestimmungen des § 15 (deutsches) Telemediengesetz (TMG) im Widerspruch zur Richtlinie 95/46/EG steht.

Entscheidung des BGH: § 15 Abs. 1 TMG ist entsprechend Art. 7 lit f der Richtlinie 95/46 EG dahin auszulegen, Anbieter von Online-Mediendiensten darf personenbezogene Daten eines Nutzers ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus verwenden darf, soweit Verwendung erforderlich ist, um generelle Funktionsfähigkeit der Dienste zu gewährleisten, es hat eine Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer zu erfolgen

VO SS2019 - Juridicum

-

Positionen und Fakten zu IP-Adresse als personenbezogene Information

öffentliche (geroutete) und private IP-Adressen:

- öffentlich: im gesamten Internet verwendbar
- private: werden für interne Netzer verwendet, können nicht im Internet verwendet werden (10.*.*.*, 193.168.*.*, ...)

genutzte und nicht-genutzte (reservierte) öffentliche IP-Adressen:

- genutzte: über WHOIS-Datenbank ist Verantwortlicher abrufbar
- reservierte: für spätere Nutzer/Verwendung reserviert

dynamische und statische IP-Adresse:

- dynamische: IP-Adresse wird von Fall zu Fall einem Teilnehmer (Vertragspartner) durch Verantwortlichen zugeordnet
- statische: IP-Adresse wird auf Dauer (etwa eines Vertragsverhältnisses) einem Teilnehmer zugeordnet (und in der WHOIS-Datenbank eingetragen)

-

Beispiele / Entscheidungen

Positionen und Fakten zu IP-Adresse als personenbezogene Information II

Unterscheidung zwischen Verantwortlichen, Teilnehmer und Nutzer:

- Verantwortlicher: in der Regel Telekomanbieter, ISP, der technische Verantgwortung trägt, jedoch keinen Einfluss darauf nimmt und auch keine Kenntnis hat, welche Informationen mittels IP-Adresse transportiert werden
- Teilnehmer: Vertragspartner des ISP, der jedoch die IP-Adresse nicht selbst benutzen muss
- Nutzer: tatsächlicher Nutzer der IP-Adresse zu einem bestimmten Zeitpunkt, er entscheidet, welche Inhalte mit der IP-Adresse transportiert werden

IP-Adresse ist KEINE personenbezogene Information:

- immer dann, wenn derjenige, der Aufzeichnungen zur IP-Adresse führt, NICHT feststellen kann/darf, wer für die transportierten Inhalte verantwortlich ist
- Beispiel: Website-Betreiber, der Zugriffe auf seine Website auf IP-Ebene loggt und nicht berechtigt ist Auskünfte beim ISP einzuholen

VO SS2019 - Juridicum

-

Positionen und Fakten zu IP-Adresse als personenbezogene Information III

IP-Adresse ist EINE personenbezogene Information:

- statische IP-Adressen sind personenbezogene Informationen, da jedermann mittels WHOIS-Datenbank den verantwortlichen Teilnehmer feststellen kann und sofern dies auch möglich ist
- alle veröffentlichen IP-Adressen zu bestimmten Nutzungen sind personenbezogene Informationen, da zumindest der **Verantwortliche (der ISP)** feststellen kann, welcher Teilnehmer diese IP-Adresse zugeordnet wurde
- alle genutzten IP-Adressen innerhalb eines internen Netzes (zB Intranet) sind personenbezogene Informationen, wenn der **Teilnehmer** feststellen kann, welcher Nutzer diese IP-Adresse zu einem bestimmten Zeitpuunkt tatsächlich genutzt hat

-

DSGVO - Grundlagen

DSGVO Art 11 "Verarbeitung ohne Identifikation"

Abs. 1: Ist zur Verarbeitung die Identifikation einer Person nicht (mehr) erforderlich, dann gibt es KEINE Verpflichtung des Verantwortlichen zur Einhaltung der DSGVO Zusatzinformationen einzuholen oder bereit zu halten

Abs. 2: Kann ein Verantwortlicher nachweisen, dass er nicht in der Lage ist einen Betroffenen zu identifizieren, sind Art. 15 bis 20 NICHT anzuwenden (Auskunfts-, Berichtigungs- und Löschungsrechte)

Jedoch!

(Abs. 2) ... außer Betroffener stellt selbst Informationen zur Identifikation zur Verfügung

ergänzende Erläuterung EW 30

Natürlichen Personen hinterlassen mittels Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen Spuren, die Identifikation ermöglichen

VO SS2019 - Juridicum

DSGVO Art. 11 Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

(1)Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.

(2)Kann der Verantwortliche in Fällen gemäß Absatz 1 des vorliegenden Artikels nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich. In diesen Fällen finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

Demobeispiele Veröffentlichung

Was ist eine zulässige Veröffentlichung?

Veröffentlichen ("offenlegen") von Informationen

- ist in DSGVO Spezialfall der Datenübermittlung
- die Veröffentlichung muss rechtlich zulässig sein

international erhebliche Wertungsunterschiede

- KFZ-Datenbank der Schweiz
  (Beispiel: http://www.viacar.ch/eindex/login.aspx?kanton=ag)
- Sexualstraftäterdatei USA
  (http://www.nsopr.gov/)
- Sexualstraftäterdatei GB
  (Google-Suche nach "schotte sex fahrrad")

Zugang zu öffentlichen Informationen wird laufend modifiziert um "Missbrauch" zu verhindern: meist **CAPTCHA** Codes verwendet = *Completely Automated Public Turing test to tell Computers and Humans Apart*

VO SS2019 - Juridicum

-

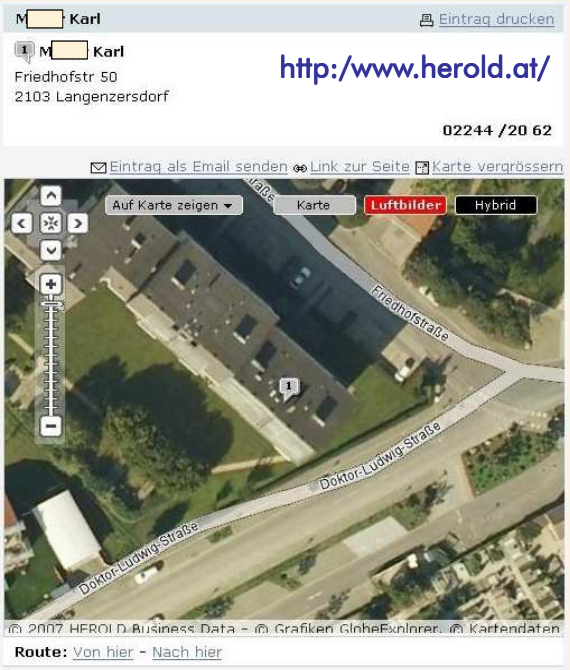
Demobeispiele Veröffentlichung

Herold verknüpft Telefonbuchsuche mit Luftbild
Fragen:
Handelt es sich bei Luftbild um personenbezogene Information?

Ist Zustimmung erforderlich?

Erfüllt Veröffentlichung berechtigten Zweck?

Wäre durch Löschung des Familiennamens Luftbild-Veröffentlichung saniert?



VO SS2019 - Juridicum

-

Was ist eine personenbezogene Veröffentlichung?

Mittwoch, 29.10.14 | 11

Inkasso-Bande schickt Unternehmer Schläger-Truppe!

Um Schulden einzutreiben, schwärzte ein Inkassobüro einen Steirer im Internet als „Betrüger" an. Ein Rollkommando stürmte sein Büro und drohte August S. (50), ihm die Kehle durchzuschneiden!

Firmenhaus wurde mit PickerIn beklebt

Nach einem gescheiterten Geschäft mit einer Firma aus Bratislava geriet Unternehmer August S. (50) aus der Steiermark ins Visier einer brutalen Inkassobande. Die Slowaken forderten 8.577 Euro von ihm.

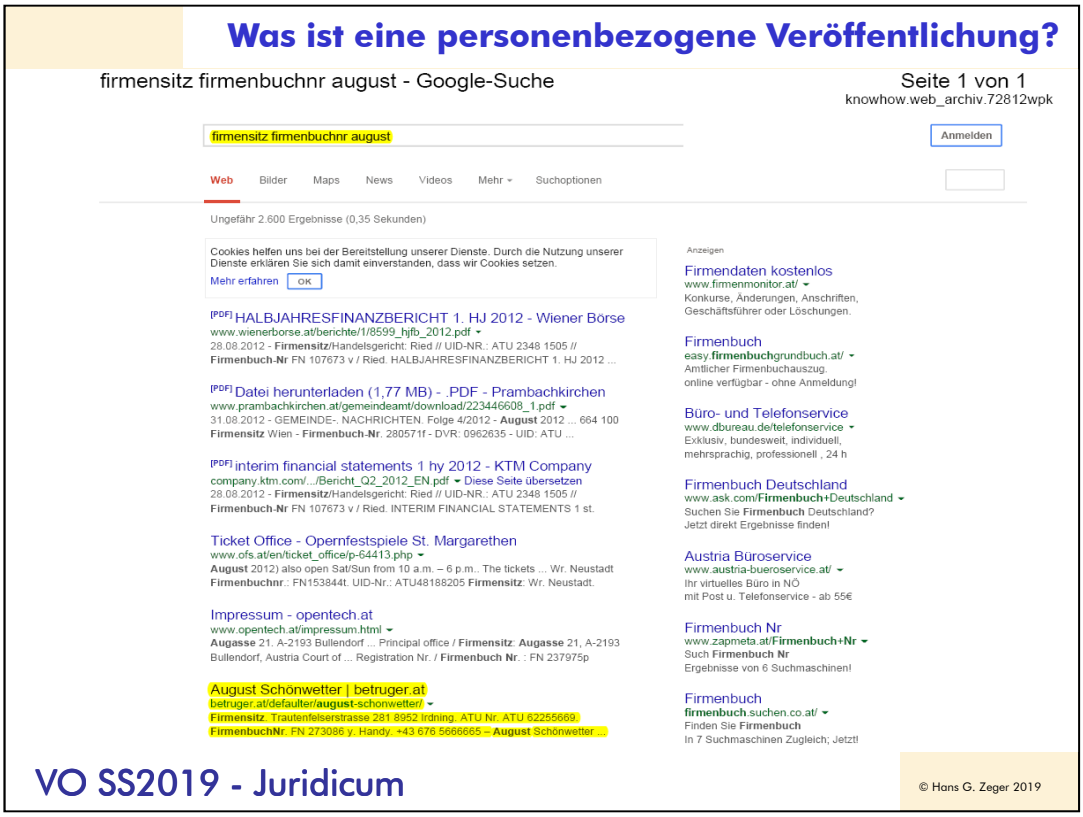
Von Thomas Peterthalner

„Ich wurde am Handy eingeschüchtert. Dabei hatte ich gar keine Schulden!" Als er nicht zahlte, wurde das Haus von August S. mit „Betruger.at"-Stickern beklebt, er selbst im Internet verunglimpft. Letzte Woche eskalierte die Situation: „Plötzlich sind zwei 120-Kilo-Männer in mein Büro gestürmt." Die Schläger drohten dem Steirer, ihm die Kehle durchzuschneiden. „Ich hatte panische Angst." August S. flüchtete aus dem Haus und rief sofort die Polizei. Die Prügler wurden festgenommen

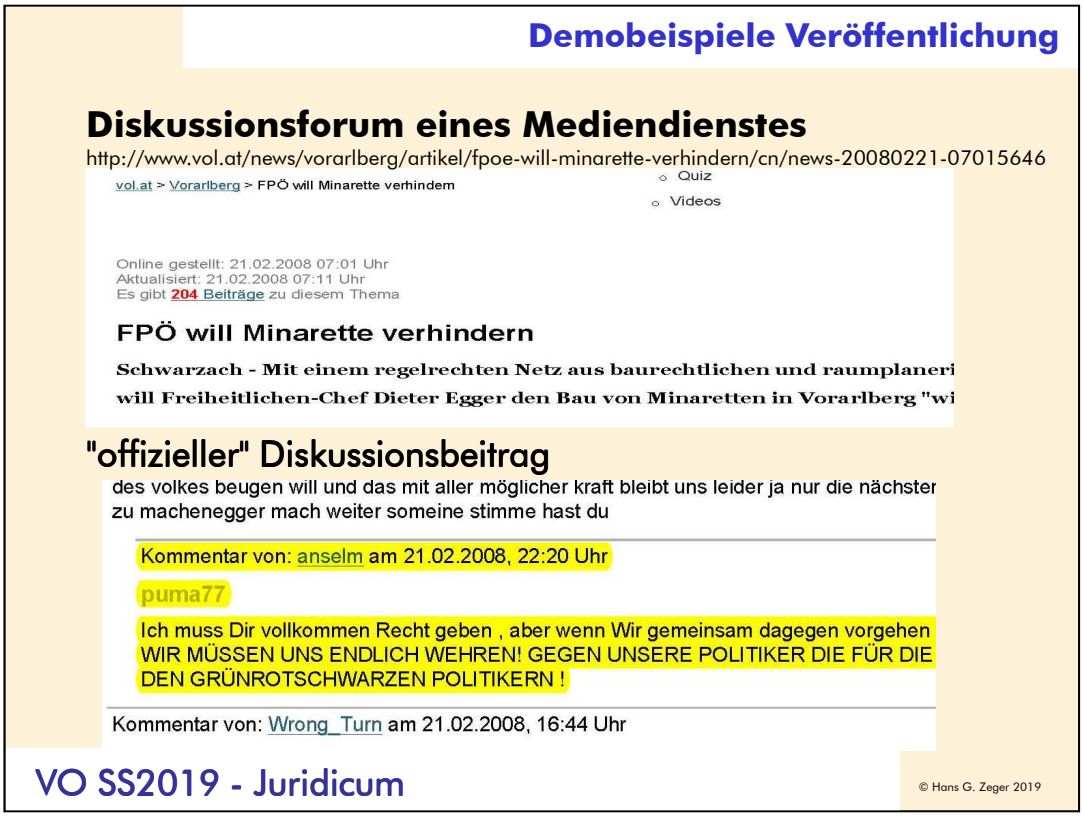
Firmen-Chef August S. wird im Netz von der Inkasso-Bande als Betrüger diffamiert.

VO SS2019 - Juridicum

-


Was ist eine personenbezogene Veröffentlichung?
firmensitz firmenbuchnr august - Google-Suche
Seite 1 von 1
knowhow.web_archiv.72812wpk
firmensitz firmenbuchnr august
Anmelden
Web Bilder Maps News Videos Mehr Suchoptionen
Ungefähr 2.600 Ergebnisse (0,35 Sekunden)
Cookies helfen uns bei der Bereitstellung unserer Dienste. Durch die Nutzung unserer Dienste erklären Sie sich damit einverstanden, dass wir Cookies setzen.
Mehr erfahren OK
[PDF] HALBJAHRESFINANZBERICHT 1. HJ 2012 - Wiener Börse
www.wienerborse.at/berichte/1/8599_hjfb_2012.pdf
28.08.2012 - Firmensitz/Handelsgericht: Ried // UID-NR.: ATU 2348 1505 // Firmenbuch-Nr FN 107673 v / Ried. HALBJAHRESFINANZBERICHT 1. HJ 2012 ...
[PDF] Datei herunterladen (1,77 MB) - .PDF - Prambachkirchen
www.prambachkirchen.at/gemeindeamt/download/223446608_1.pdf
31.08.2012 - GEMEINDE-. NACHRICHTEN. Folge 4/2012 - August 2012 ... 664 100 Firmensitz Wien - Firmenbuch-Nr. 280571f - DVR: 0962635 - UID: ATU ...
[PDF] interim financial statements 1 hy 2012 - KTM Company
company.ktm.com/.../Bericht_Q2_2012_EN.pdf Diese Seite übersetzen
28.08.2012 - Firmensitz/Handelsgericht: Ried // UID-NR.: ATU 2348 1505 // Firmenbuch-Nr FN 107673 v / Ried. INTERIM FINANCIAL STATEMENTS 1 st.
Ticket Office - Opernfestspiele St. Margarethen
www.ofs.at/en/ticket_office/p-64413.php
August 2012) also open Sat/Sun from 10 a.m. – 6 p.m.. The tickets ... Wr. Neustadt Firmenbuchnr.: FN153844t. UID-Nr.: ATU48188205 Firmensitz: Wr. Neustadt.
Impressum - opentech.at
www.opentech.at/impressum.html
Augasse 21. A-2193 Bullendorf ... Principal office / Firmensitz: Augasse 21, A-2193 Bullendorf, Austria Court of ... Registration Nr. / Firmenbuch Nr. : FN 237975p
August Schönwetter | betruger.at
betruger.at/defaulter/august-schonwetter/
Firmensitz: Trautenfelserstrasse 281 8952 Irdning. ATU Nr. ATU 62255669 . FirmenbuchNr. FN 273086 y. Handy. +43 676 5666665 – August Schönwetter ...
Anzeigen
Firmendaten kostenlos
www.firmenmonitor.at/
Konkurse, Änderungen, Anschriften, Geschäftsführer oder Löschungen.
Firmenbuch
easy.firmenbuchgrundbuch.at/
Amtlicher Firmenbuchauszug. online verfügbar - ohne Anmeldung!
Büro- und Telefonservice
www.dbureau.de/telefonservice
Exklusiv, bundesweit, individuell, mehrsprachig, professionell , 24 h
Firmenbuch Deutschland
www.ask.com/Firmenbuch+Deutschland
Suchen Sie Firmenbuch Deutschland? Jetzt direkt Ergebnisse finden!
Austria Büroservice
www.austria-bueroservice.at/
Ihr virtuelles Büro in NÖ mit Post u. Telefonservice - ab 55€
Firmenbuch Nr
www.zapmeta.at/Firmenbuch+Nr
Such Firmenbuch Nr Ergebnisse von 6 Suchmaschinen!
Firmenbuch
firmenbuch.suchen.co.at/
Finden Sie Firmenbuch In 7 Suchmaschinen Zugleich; Jetzt!
VO SS2019 - Juridicum
© Hans G. Zeger 2019

-



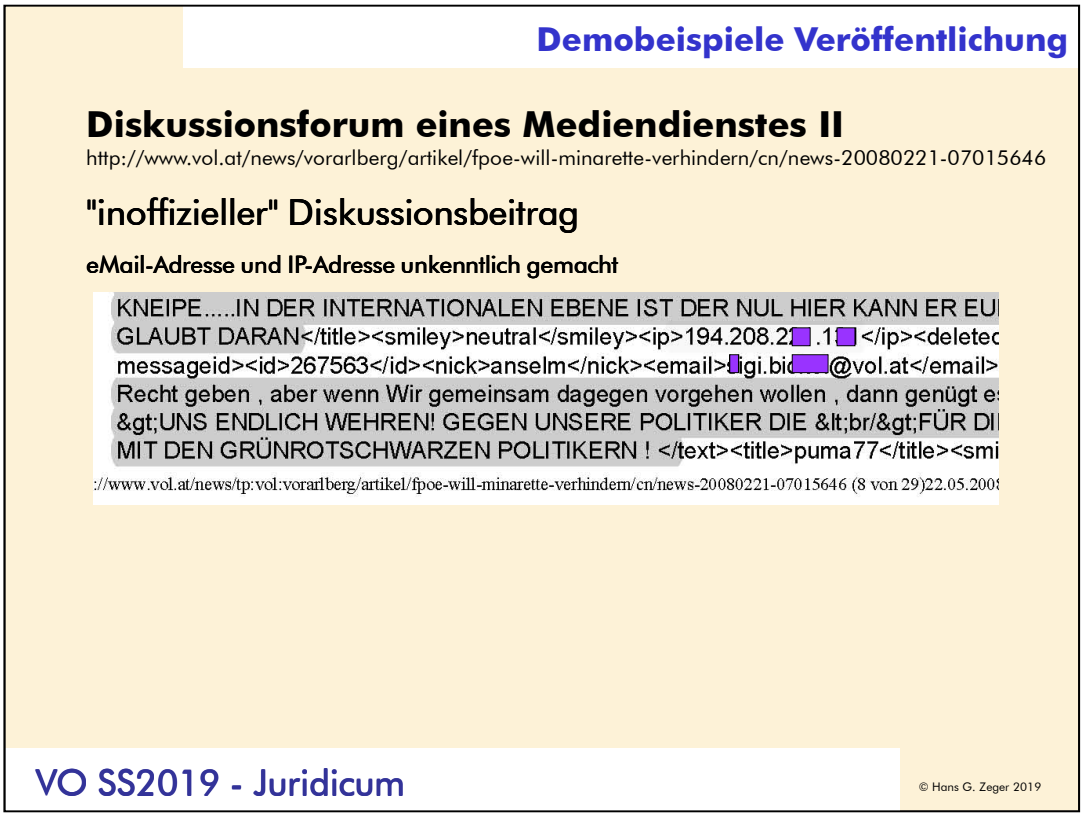
Offizielle Version:

Kommentar von: anselm am 21.02.2008, 22:20 Uhr

puma77

Ich muss Dir vollkommen Recht geben , aber wenn Wir gemeinsam dagegen vorgehen wollen , dann genügt es nicht die nächsten Wahlen abzuwarten!

WIR MÜSSEN UNS ENDLICH WEHREN! GEGEN UNSERE POLITIKER DIE FÜR DIE ISLAMISIERUNG IN ÖSTERREICH SIND !!!!!ZUM TEUFEL MIT DEN GRÜNROTSCHWARZEN POLITIKERN !



"Inoffizielle" Version:

FÜR KLEIN POLITIK DER WO KEINEN VISION HAT ALTFRAUEN LABER MACHT IN EINEN STAMM KUNDEN TISCH IRGEND EINER DRIT KLASSIGE KNEIPE.....IN DER INTERNATIONALEN EBENE IST DER NUL HIER KANN ER EUREN EGO BEFRIEDIGEN !!!SO IST DAS EBEN </text><title>UND IHR

GLAUBT DARAN</title>
<smiley>neutral</smiley><ip>**194.208.2XX.1XX**</ip><deleted>0</deleted></mess age><message><messageid>162</messageid><id>267563</id><nick>anselm< /nick><email>**XXgi.bicXXX@vol.at**</email><date>2008-02-21T22:20:48.873</date><text>Ich muss Dir vollkommen Recht geben , aber wenn Wir gemeinsam dagegen vorgehen wollen, dann genügt es
nicht die nächsten Wahlen abzuwarten! WIR MÜSSEN
UNS ENDLICH WEHREN! GEGEN UNSERE POLITIKER DIE
FÜR DIE ISLAMISIERUNG IN ÖSTERREICH SIND !!!!!ZUM
TEUFEL MIT DEN GRÜNROTSCHWARZEN POLITIKERN ! </text><title>puma77</title>
<smiley>neutral</smiley><ip>**194.208.2XX.5X**</ip><replyid>139</

- Werden personenbezogene Daten veröffentlicht (fehlerhafte/offizielle Version)?
- Handelt es sich um eine Datenanwendung im Sinne des DSG?
- Besteht eine Rechtsgrundlage für die Veröffentlichung?
  (berechtigter Zweck, zulässige Datenverwendung, Registrierung)

Demobeispiele Veröffentlichung

Diskussionsforum eines Mediendienstes III

- Werden personenbezogene Daten veröffentlicht (fehlerhafte/offizielle Version)?
- Handelt es sich um eine Datenverarbeitung im Sinne des DSGVO?
- Besteht eine Rechtsgrundlage für die Veröffentlichung? (berechtigter Zweck, zulässige Datenverwendung, Registrierungserfordernis)
- Welche Bestimmungen/Regulierungen sind anzuwenden?
- Verhalten bei Kenntnisnahme durch Internetbenutzer?
- Wer ist für Aufsicht verantwortlich / Welche Zuständigkeit?
- Welche Sanktionen sind vorgesehen?

VO SS2019 - Juridicum

-

Demobeispiele Veröffentlichung

http://www.sexpunkt.at/ [Website seit 2011 nicht mehr aktiv]

VO SS2019 - Juridicum

-

Demobeispiele Veröffentlichung

öffentlich zugängliche Besucherstatistik zu sexpunkt.at

20.	29 April	17:51	Hutchison 3G Austria GmbH, Wampersdorf, Niederosterreich, Österreich
21.	29 April	18:36	Highway Customers, Villach, Karnten, Österreich
22.	29 April	18:37	Highway Customers, Villach, Karnten, Österreich
23.	29 April	19:01	Highway Customers, Innsbruck, Tirol, Österreich
24.	29 April	19:02	Highway Customers, Innsbruck, Tirol, Österreich
25.	29 April	20:57	T-Mobile Austria GmbH, Vienna, Wien, Österreich
26.	29 April	20:58	T-Mobile Austria GmbH, Vienna, Wien, Österreich
27.	29 April	20:59	T-Mobile Austria GmbH, Vienna, Wien, Österreich
28.	30 April	10:07	Arcor AG, Berlin, Deutschland
29.	30 April	14:12	TELEZUG AG, Zug, Schweiz
30.	30 April	21:46	Bundesministerium fuer Inneres, Vienna, Wien, Österreich
31.	1 Mai	09:55	Chello Broadband GmbH, Innsbruck, Tirol, Österreich
32.	1 Mai	15:17	Inode Internet, Sierning, Oberosterreich, Österreich
33.	1 Mai	15:18	Inode Internet, Sierning, Oberosterreich, Österreich

Besucherkarte

VO SS2019 - Juridicum

- Werden personenbezogene Daten veröffentlicht Version)?
- Handelt es sich um eine Datenanwendung im Sinne des DSG?
- Besteht eine Rechtsgrundlage für die Veröffentlichung?
  (berechtigter Zweck, zulässige Datenverwendung, Registrierung)

Demobeispiele Veröffentlichung

öffentlich zugängliche Besucherstatistik zu "zärtliche Nicole"
http://zaertliche-nicole.com/ [Counter 2011 nicht mehr aktiv]

3.	30 April	21:26	LIWEST Kabelfernsehen Errichtungs- und Betriebs Ge, Linz, Oberosterreich, Österreich
4.	30 April	21:32	Chello Broadband GmbH, Vienna, Wien, Österreich
5.	30 April	22:21	Juergen I[redacted]t, Vienna, Wien, Österreich
6.	30 April	22:51	Highway Customers, Mattersburg, Burgenland, Österreich
7.	30 April	22:52	Highway Customers, Vienna, Wien, Österreich
8.	30 April	23:01	Kabelsignal AG, Baden, Niederosterreich, Österreich
9.	30 April	23:04	Chello Broadband GmbH, Vienna, Wien, Österreich
10.	30 April	23:12	Telecom Italia, Bolzano, Trentino-Alto Adige, Italien
11.	30 April	23:19	Kabelsignal AG, Gumpoldskirchen, Niederosterreich, Österreich
12.	30 April	23:21	Chello Broadband GmbH, Vienna, Wien, Österreich
13.	30 April	23:37	Highway Customers, Vienna, Wien, Österreich
14.	30 April	23:47	Highway Customers, Vienna, Wien, Österreich
15.	1 Mai	00:08	Chello Broadband GmbH, Vienna, Wien, Österreich
16.	1 Mai	00:30	Hausservice-Objekterrichtungs- u. Bewirtschaftungs, Vienna, Wien, Österreich
17.	1 Mai	00:34	Highway Customers, Krems, Niederosterreich, Österreich
18.	1 Mai	01:40	MobilePools, Vienna, Wien, Österreich

VO SS2019 - Juridicum

-

Googles Street-View

Aufzeichnung "öffentlichen" Verhaltens

http://maps.google.com/help/maps/streetview

- handelt es sich überhaupt um personenbezogene Datenverarbeitung?
- Google sagt zu, Personen vor Veröffentlichung zu "verpixeln"
- Was ist zu den Street-View-Funseiten zu sagen?
  http://www.streetviewfun.com/ http://streetviewr.com/

VO SS2019 - Juridicum

-

Googles Street-View

DSK genehmigt 2011 Street-View Anwendung
mit drei Empfehlungen (K213.120/0002-DSK/2012 14.2.2012)

- Aufnahmen von Personen in sensiblen Bereichen sind die Gesamtbilder der Personen unkenntlich zu machen: etwa Eingangsbereiche von Kirchen, Gebetshäusern, Krankenhäusern, Frauenhäusern und Gefängnissen
- für Spaziergänger nicht einsehbare Immobilien (umzäunte Privatgärten und -höfe) sind vor Veröffentlichung im Internet unkenntlich zu machen
- Schaffung eines einfachen Widerspruchsrechts nach § 28 Abs. 2 DSG 2000

VO SS2019 - Juridicum

-

Social Media und Datenschutz

Datenschutzspezifische Fragestellungen

Vorgaben DSGVO:

(1) Rollenkonzept: Verantwortlicher, Betroffener, Auftragsverarbeiter
(2) Schutzinteressen der persönlichen Daten: allgemein verfügbare Daten, indirekt personenbezogene Daten, vertrauliche Daten, sensible Daten
(3) berechtigter Zweck: der persönlichen Nutzung, die Weitergabe an Dritte, Veröffentlichung
(4) Aufsicht: keine generelle Aufsicht, mögliche Genehmigung internationaler Datenverkehr / Konsultation Datenschutzfolgenabschätzung erforderlich

Datenschutzregeln treffen sowohl Betreiber des Accounts ("Benutzer" [A]), als auch Plattformbetreiber ("Facebook" [B]),

VO SS2019 - Juridicum

-

Social Media und Datenschutz

Variante: Unternehmen ("Benutzer") richtet (Facebook-) Account ein und berichtet öffentlich über sich und erlaubt Dritten Beiträge beizusteuern

(1) Rollenkonzept:

[A] Benutzer ist bezüglich der veröffentlichten Daten Dritter Verantwortlicher, Facebook ist in diesem Fall Auftragsverarbeiter, Datenverarbeitung liegt vor!

[B] Im Zusammenhang mit den Zugangsdaten und bei eigenverantwortlicher Verwertung von Benutzerdaten (z.B. für Online-Marketingzwecke) ist Facebook Verantwortlicher

VO SS2019 - Juridicum

-

Social Media und Datenschutz

Variante: Unternehmen ("Benutzer") richtet (Facebook-) Account ein und berichtet öffentlich über sich und erlaubt Dritten Beiträge beizusteuern

(2) Schutzinteresse:

[A] Bezüglich der Veröffentlichung der Unternehmensdaten gilt, kein Schutzinteresse, da Benutzer seine Daten selbst veröffentlicht hat, bezüglich Dritter (Poster + Person über die gepostet wird) hat Unternehmen auf Einhaltung der Datenschutzinteressen zu achten! Es sind zusätzlich zu DSGVO die ECG-Bestimmungen insb. § 16 (Haftung!) zu beachten.

[B] Facebook darf die Daten nur im Rahmen der ausdrücklich vereinbarten Geschäftsbedingungen verwenden.

VO SS2019 - Juridicum

-

Social Media und Datenschutz

Variante: Unternehmen ("Benutzer") richtet (Facebook-) Account ein und berichtet öffentlich über sich und erlaubt Dritten Beiträge beizusteuern

(3) Berechtigter Zweck:

[A] Keine private Datenverarbeitung im Sinne DSGVO Art. 2, jedoch in der Regel zulässig (z.B. Unternehmenspräsentation, Erwerbsfreiheit).

[B] In Bezug auf Facebook aus Angebot und Geschäftsbedingungen ableitbar.

(4) Aufsicht:

[A] Für Unternehmen mit Sitz in EU in der Regel keine vorbeugende Aufsicht

[B] Für Facebook gelten die Bestimmungen des Geschäftssitzes

[C] Zuständigkeit der Datenschutzbehörde des jeweiligen EU-Staates falls sich Dienst an Bürger "mit Aufenthalt in EU" wendet

[D] sind mehrere EU-Staaten betroffen, greift Konsulationsmechanismus

VO SS2019 - Juridicum

-

Beispiele / Entscheidungen

Ist eine Suchmaschine eine Datenverarbeitung im Sinne der DSGVO?

Ausgangslage

- Immobilie eines Spaniers in Geldnöten wurde öffentlich zur Versteigerung angeboten
- Versteigerung in lokalem Medium öffentlich bekannt gemacht (auch in Online-Version im Internet)
- Jahre später findet Spanier diesen Eintrag üebr Suchmaschine Google, verlangt Löschung bei Medium und Google
- spanische Datenschutzbehörde erklärt sich sowohl für Google, als auch Medium zuständig
- keine Löschung bei Medium (Meinungsfreiheit), jedoch keine Anzeige bei Google
- Google klagt, es kommt zum Vorabentscheidungsverfahren bei EuGH

VO SS2019 - Juridicum

Urteil C131/12 13. Mai 2014

Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 2 Buchst. b und d, Art. 4 Abs. 1 Buchst. a und c, Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281, S. 31) sowie von Art. 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).

Es ergeht im Rahmen eines Rechtsstreits zwischen der Google Spain SL (im Folgenden: Google Spain) und der Google Inc. auf der einen Seite und der Agencia Española de Protección de Datos (AEPD) (spanische Datenschutzagentur, im Folgenden: AEPD) und Herrn Costeja González auf der anderen Seite über eine Entscheidung der AEPD, mit der einer von Herrn Costeja González gegen die beiden genannten Gesellschaften erhobenen Beschwerde stattgegeben und Google Inc. angewiesen wurde, die erforderlichen Maßnahmen zu ergreifen, um Herrn Costeja González betreffende personenbezogene Daten aus ihrem Index zu entfernen und den Zugang zu diesen Daten in Zukunft zu verhindern.

Beispiele / Entscheidungen

Ist eine Suchmaschine eine Datenverarbeitung im Sinne der DSGVO? II

EuGH-Entscheidung C131/12 Costeja González **13. Mai 2014**

- Europäisches Recht ist anzuwenden, auch wenn Verarbeitung außerhalb EU erfolgt, lokale (nationale) Werbeaktivitäten für Google-Seite in EU ist ausreichend
- Suchindex ist als Datenverarbeitung iS der EG-Richtlinie zu verstehen
- Privatsphäre ist höher zu bewerten als Verwertungsinteresse durch Google
- kein absoluter Löschungsanspruch, sondern Abwägung von öffentlichem Interesse und Privatsphäre

Anmerkungen

- schon bisher unterbindet Google die Anzeige aus zahllosen Gründen (u.a. nationale Gesetze, noindex-Einträge, Vereinbarungen mit Rechteinhabern, ...)
- unklar sind Grenzen der Abwägung und Umfang des nationalen Google-Engagements

VO SS2019 - Juridicum

Urteil C131/12 13. Mai 2014 - Begründung

Art. 2 Buchst. b und d der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, sofern die Informationen personenbezogene Daten enthalten, als „Verarbeitung personenbezogener Daten" im Sinne von Art. 2 Buchst. b der Richtlinie 95/46 einzustufen ist und dass der Betreiber dieser Suchmaschinen als für diese Verarbeitung „Verantwortlicher" im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 anzusehen ist.

Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 ist dahin auszulegen, dass im Sinne dieser Bestimmung eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung ausgeführt wird, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt, wenn der Suchmaschinenbetreiber in einem Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst eine Zweigniederlassung oder Tochtergesellschaft gründet, deren Tätigkeit auf die Einwohner dieses Staates ausgerichtet ist.

Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 sind dahin auszulegen, dass der Suchmaschinenbetreiber zur Wahrung der in diesen Bestimmungen vorgesehenen Rechte, sofern deren Voraussetzungen erfüllt sind, dazu verpflichtet ist, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links zu von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person zu entfernen, auch wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden und gegebenenfalls auch dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist.

Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 sind dahin auszulegen, dass im Rahmen der Beurteilung der Anwendungsvoraussetzungen dieser Bestimmungen u. a. zu prüfen ist, ob die betroffene Person ein Recht darauf hat, dass die Information über sie zum gegenwärtigen Zeitpunkt nicht mehr durch eine Ergebnisliste, die im Anschluss an eine anhand ihres Namens durchgeführte Suche angezeigt wird, mit ihrem Namen in Verbindung gebracht wird, wobei die Feststellung eines solchen Rechts nicht voraussetzt, dass der betroffenen Person durch die Einbeziehung der betreffenden Information in die Ergebnisliste ein Schaden entsteht. Da die betroffene Person in Anbetracht ihrer Grundrechte aus den Art. 7 und 8 der Charta verlangen kann, dass die betreffende Information der breiten Öffentlichkeit nicht mehr durch Einbeziehung in eine derartige Ergebnisliste zur Verfügung gestellt wird, überwiegen diese Rechte grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit am Zugang zu der Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche. Dies wäre jedoch nicht der Fall, wenn sich aus besonderen Gründen – wie der Rolle der betreffenden Person im öffentlichen Leben – ergeben sollte, dass der Eingriff in die Grundrechte dieser Person durch das überwiegende Interesse der breiten Öffentlichkeit daran, über die Einbeziehung in eine derartige Ergebnisliste Zugang zu der betreffenden Information zu haben, gerechtfertigt ist.

Beispiele / Entscheidungen

Weitere Themen

DSK 120.881/010-DSK/2003 12.12.2003
("eMail-Datenverarbeitung")

Auch e-Mail-Verkehr ist als Datenverarbeitung iS des DSG 2000 anzusehen und unterliegt der Auskunftspflicht

DSB-D123.077/0003-DSB/2018 13.8.2018
("Löschung von Online-Postings")

DSB bejaht grundsätzlich die Anwendbarkeit der DSGVO, sieht aber keine Zuständigkeit, da Postings bei einem Online-Medium unter das "Medienprivileg" des DSG fällt - *rechtskräftig*

DSB-D122.984/0003-DSB/2018 3.12.2018
("Veröffentlichung eines Jagdbescheids auf Naturschutzblog")

DSB bejaht Zuständigkeit und trägt Entfernung auf - *nicht rechtskräftig*

VO SS2019 - Juridicum

-

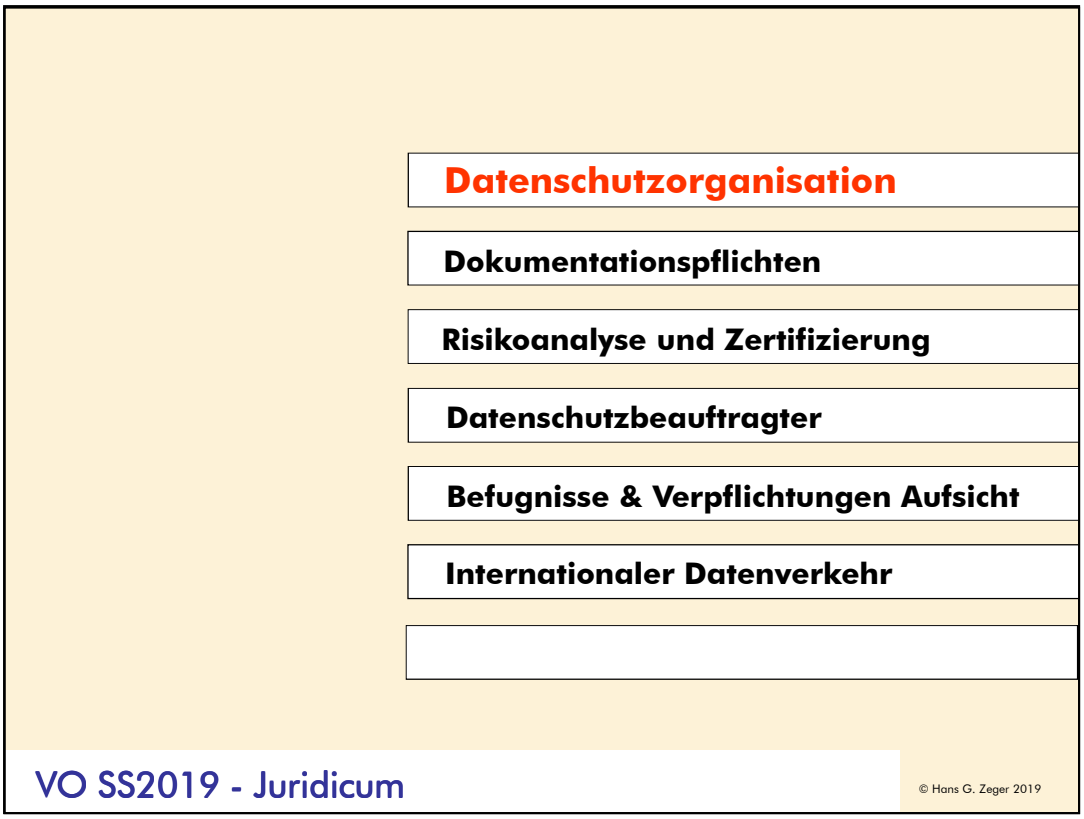
Beispiele / Entscheidungen

In welchem Umfang sind DSG/DSGVO auf das Internet anwendbar?

- Fällt eine Veröffentlichung auf einer **Internetseite** unter die Bestimmungen der Datenschutzrichtlinie? (**ja**, siehe EuGH C-101/01 Lindqvist)
- Wann handelt es sich um **personenbezogene** Daten?
  Name, Adresse, Identifikationsdaten
  eMail-Adresse (**ja**, siehe OLG Bamberg/D 1U143/04 12.5.2005)
  IP-Adresse (**ja**, siehe EuGH Breyer C-582/14)
  Kundennummer/Benutzerkennung, Cookies, personalisierte/anonymisierte Webinformationen, ...
  Kriterium ist "Identifizierbarkeit" (iS DSGVO Art. 4 Abs 1 + Art. 11)
- **wirtschaftliche Interessen (Werbeverkauf)** vs. Privatsphäre?
  (EuGH C131/12 Google-Spain-Entscheidung)
- Medienprivileg vs. Privatsphäre
  (grundsätzliche Anwendbarkeit, offen Ausnahmen, Zuständigkeit DSB-D123.077/0003-DSB/2018 13.8.2018, DSB-D122.984/0003-DSB/2018 3.12.2018)
- Ist **eMail-Verkehr** eine **Datenverarbeitung**?
  (**ja**, siehe DSK K120.881/010-DSK/2003 12.12.2003, ...)

VO SS2019 - Juridicum

-


Datenschutzorganisation
Dokumentationspflichten
Risikoanalyse und Zertifizierung
Datenschutzbeauftragter
Befugnisse & Verpflichtungen Aufsicht
Internationaler Datenverkehr
VO SS2019 - Juridicum
© Hans G. Zeger 2019

-

DSGVO - Datenschutzorganisation

DSGVO Art. 30
"Verzeichnis der Verarbeitungstätigkeiten"

Verzeichnis ist von folgenden Verantwortlichen zu führen:
(es genügt, wenn eine Bedingung zutrifft!)

- Einrichtungen mit mehr als 250 Mitarbeitern
- weniger als 250 Mitarbeiter, wenn Verarbeitung mehr als "gelegentlich" erfolgt
- Datenverarbeitung birgt besondere Risken für Betroffene [Anm. werden Informationsdienste, Profiling-Verarbeitungen sein]
- Verantwortliche verarbeiten besondere Kategorien von Daten (Art. 9 Abs. 1)
- Verantwortliche verarbeiten strafrechtliche Verurteilungen und Straftaten (Art. 10)

Inhalt des Verzeichnisses (soweit zutreffend):

- Namen und Kontaktdaten des Verantwortlichen, seines Vertreters und seines Datenschutzbeauftragten

VO SS2019 - Juridicum

DSGVO Art. 30 Verzeichnis von Verarbeitungstätigkeiten

(1)Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(2)Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

DSGVO - Datenschutzorganisation

DSGVO Art. 30
"Verzeichnis der Verarbeitungstätigkeiten" II

- Zwecke der Verarbeitung
- Beschreibung der Kategorien der verwendeten Daten
- Kategorien der Empfänger (inklusive innerbetriebliche Empfänger) gegenüber denen Daten offengelegt wurden oder werden (einschließlich Drittländer oder internationale Organisationen)
- Dokumentation der Garantien im Fall von Übermittlungen in Drittländer oder an internationale Organisationen
- "wenn möglich" [?] vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien
- "wenn möglich" [?] allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32

Ähnliches Verzeichnis hat auch Auftragsverarbeiter zu führen

Verzeichnis ist schriftlich zu führen (elektronisch ist zulässig)

Verzeichnis ist auf Verlangen der Aufsichtsbehörde vorzulegen

VO SS2019 - Juridicum

DSGVO Art. 30 Verzeichnis von Verarbeitungstätigkeiten (Fortsetzung)

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(3)Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4)Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(5)Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

DSGVO - Datenschutzorganisation

DSGVO Art. 35 "Datenschutz-Folgenabschätzung"

allgemeine Voraussetzungen zum Führen einer Folgenabschätzung (DPIA, DSFA):
jede Form der Verarbeitung mit hohem Risiko für die Rechte und Freiheiten natürlicher Personen

- ✓ Verwendung neuer Technologien
  [Anm.: heuristische Verfahren, CRM-Analysen, "Big-Data"-Analysen, statistische Verfahren, Verfahren mit "hohen" FAR/FRR-Ergebnissen]
- ✓ besonders umfangreiche Datenverarbeitungen
  [Anm.: "alle" Personen einer Gruppe]
- ✓ besondere Umstände der Datenverarbeitung
  [Anm.: mangelnde Freiwilligkeit, besonders exponierte Personengruppe, etwa im Sozialbereich, unscharf abgegrenzte Betroffenengruppe]
- ✓ besondere Zwecke der Datenverarbeitung
  [Anm.: Verarbeitungsergebnis hat weitreichende Konsequenzen, zB Job-Verlust, Verlust einer Berechtigung, Terminverlust, ...]

VO SS2019 - Juridicum

DSGVO Art. 35 Datenschutz-Folgenabschätzung

(1) 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 führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

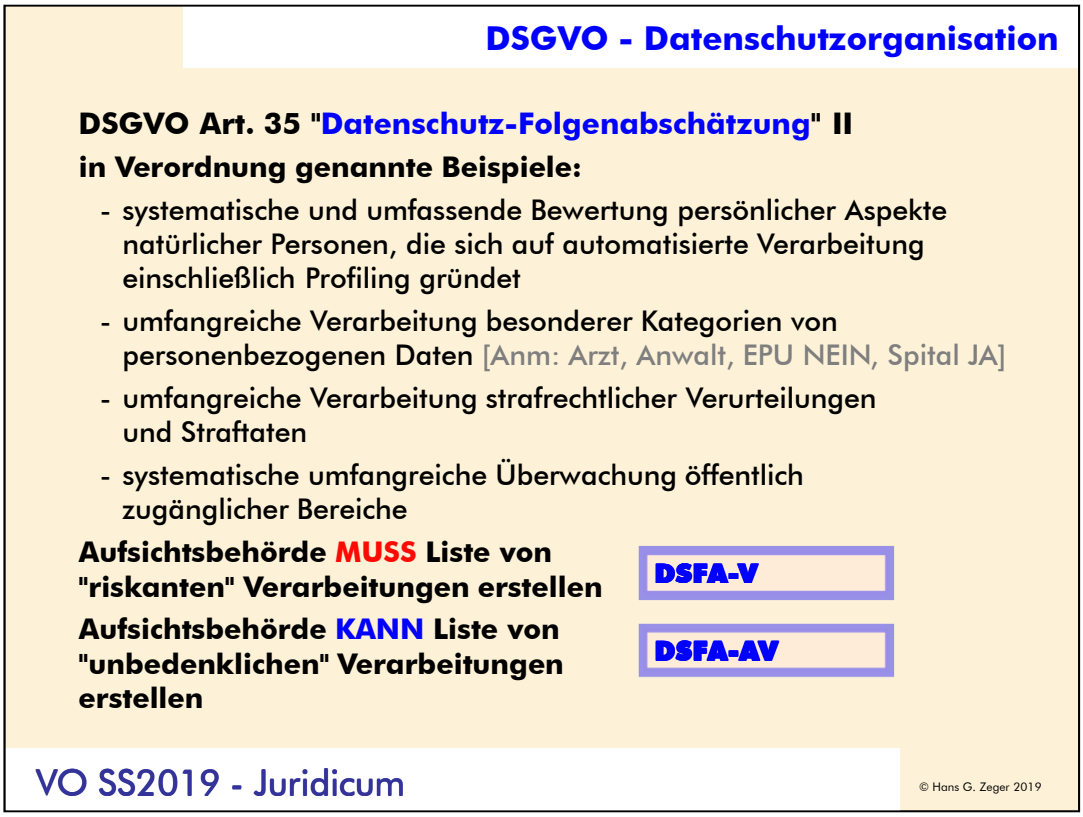
(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz- Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.



DSGVO Art. 35 Datenschutz-Folgenabschätzung (Fortsetzung)

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

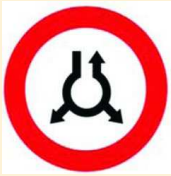
DSGVO - Datenschutzorganisation

DSGVO Art. 35 "Datenschutz-Folgenabschätzung" III

Listen müssen im "Kohärenzverfahren" mit den anderen EU-Staaten abgestimmt werden

Inhalt der Folgenabschätzung (soweit zutreffend):

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, einschließlich der vom Verantwortlichen verfolgten berechtigten Interessen
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird



VO SS2019 - Juridicum

-

DSGVO - Datenschutzorganisation

DSFA-AV "Datenschutz-Folgenabschätzung" IV
Stand 25.5.2018: Verordnung
Keine Folgenabschätzung (Auszug):
DSFA-A03 Mitgliederverwaltung [**]
DSFA-A04 Kundenbetreuung und Marketing für eigene Zwecke [**]
DSFA-A07 Zugriffsverwaltung für EDV-Systeme [**]
DSFA-A08 Zutrittskontrollsysteme [BIOM]
DSFA-A09 Stationäre Bildverarbeitung [**]
DSFA-A10 Bild- und Akustikdatenverarbeitung in Echtzeit [**]
DSFA-A12 Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter und Apotheker [**]
DSFA-A13 Rechts- und Beratungsberufe [EINZEL]
DSFA-A15 Unterstützungsbekundungen im Rahmen von Bürgerinitiativen [**]
DSFA-A18 Förderverwaltung [BES]
[**]: keine Einschränkung Datenarten
[BES]: kein Verarbeitung besonderer Datenkategorien oder strafrechtliche Daten
[BIOM]: nicht bei biometrischen Daten, Bilder sind KEINE biometrische Daten
[EINZEL]: generelle Ausnahme für alle Tätigkeiten bei Einzeltätigkeit
Orientierung an alter Standard- und Musterverordnung

VO SS2019 - Juridicum

DSFA-AV - Übersicht:

DSFA-A01 Kundenverwaltung, Rechnungswesen, Logistik, Buchführung
DSFA-A02 Personalverwaltung für privatrechtliche und öffentlich-rechtliche Dienstverhältnisse
DSFA-A03 Mitgliederverwaltung
DSFA-A04 Kundenbetreuung und Marketing für eigene Zwecke
DSFA-A05 Sach- und Inventarverwaltung
DSFA-A06 Register, Evidenzen, Bücher
DSFA-A07 Zugriffsverwaltung für EDV-Systeme
DSFA-A08 Zutrittskontrollsysteme
DSFA-A09 Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung)
DSFA-A10 Bild- und Akustikdatenverarbeitung in Echtzeit
DSFA-A11 Bild- und Akustikverarbeitungen zu Dokumentationszwecken
DSFA-A12 Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter und Apotheker
DSFA-A13 Rechts- und Beratungsberufe
DSFA-A14 Wissenschaftliche Forschung und Statistik
DSFA-A15 Unterstützungsbekundungen im Rahmen von Bürgerinitiativen
DSFA-A16 Haushaltsführung der Gebietskörperschaften und sonstigen juristischen Personen öffentlichen Rechts
DSFA-A17 Öffentliche Abgabenverwaltung
DSFA-A18 Förderverwaltung
DSFA-A19 Öffentlichkeitsarbeit und Informationstätigkeit durch öffentliche Funktionsträger und deren Geschäftsapparate
DSFA-A20 Aktenverwaltung (Büroautomation) und Verfahrensführung
DSFA-A21 Organisation von Veranstaltungen

DSGVO - Datenschutzorganisation

DSFA-V "Datenschutz-Folgenabschätzung" V

Verordnung enthält keine Liste von Verarbeitungen, sondern wiederholt im Wesentlichen die allgemeinen Vorgaben der DSGVO

In den Erläuterungen werden beispielhaft Fälle aufgezählt, die schon von der Art. 29 - Gruppe (jetzt "Europäsicher Datenschutz-Ausschuss) genannt wurden

Zwischen DSFA-AV und DSFA-V bleibt weiterhin ein (überflüssig) großer Graubereich bei der der Verantwortliche selbst entscheiden muss, ob er eine Folgenabschätzung macht oder nicht

Folgenabschätzung verpflichtend (Beispiele aus Erläuterungen):

- Verarbeitungsvorgänge im Zusammenhang mit Bonitätsdatenbanken bei Vertragsabschlüssen/-änderungen
- Kreditinstitute, die Datenbanken von Kreditauskunfteien im Rahmen von Geldwäsche, Betrug, Terrorismusbekämppfung usw durchsuchen
- Anbieter von Gentests an Betroffene
- Unternehmen die Online-Tracking betreiben (ausgenommen ausschließlich Werbung)
- Dating-Portale die Benutzerprofile erstellen
- BIG DATA Analysen

VO SS2019 - Juridicum

DSFA-V - Entwurf:

Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist

§ 2. (1) Sofern die Verarbeitung rechtmäßig im Sinne des Art. 6 DSGVO erfolgt und keine Datenverarbeitung gemäß der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl. II Nr. 108/2018, vorliegt, ist nach Maßgabe der folgenden Bestimmungen jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen.

(2) Eine Datenschutz-Folgenabschätzung ist durch den Verantwortlichen durchzuführen, wenn ein in Z 1 bis Z 7 genanntes Kriterium erfüllt ist:

1. Verarbeitungen, die eine Bewertung oder Einstufung natürlicher Personen – einschließlich des Erstellens von Profilen und Prognosen – umfassen für Zwecke, welche die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben und Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen und negative rechtliche, physische oder finanzielle Auswirkungen haben können.

2. Verarbeitungen von Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von natürlichen Personen dienen und von Dritten dazu genutzt werden können, automatisierte Entscheidungsfindungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen.

3. Verarbeitungsvorgänge, welche die Beobachtung, Überwachung oder Kontrolle von Betroffenen – insbesondere mittels Bild- und damit verbundenen Akustikdatenverarbeitungen – zum Ziel haben und

a) über Netzwerke erfasste Daten betreffen oder auf eine systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche abzielen,

b) öffentliche Orte, die gemäß § 27 Abs. 2 Sicherheitspolizeigesetz – SPG, BGBl. Nr. 566/1991, von einem nicht von vornherein bestimmten Personenkreis betreten werden können, erfassen,

c) Straßen mit öffentlichem Verkehr, die gemäß § 1 Straßenverkehrsordnung 1960 (StVO 1960), BGBl. Nr. 159/1960, von jedermann unter den gleichen Bedingungen benützt werden können, erfassen,

d) Örtlichkeiten, welche aufgrund eines Kontrahierungszwanges von jedermann betreten werden dürfen, erfassen,

e) Örtlichkeiten, welche aufgrund des öffentlichen Interesses von jedermann betreten werden dürfen, erfassen,

f) unter Einsatz von mobilen Kameras zum Zweck der Vorbeugung oder Abwehr gefährlicher Angriffe im öffentlichen und nichtöffentlichen Raum erfolgen,

g) Bild- und Akustikverarbeitungen umfassen, die dem vorbeugenden Schutz von Personen oder Sachen auf privaten, zu Wohnzwecken dienenden Liegenschaften dienen, die nicht ausschließlich vom Verantwortlichen und von allen im gemeinsamen Haushalt lebenden Nutzungsberechtigten genutzt werden, oder

DSGVO - Datenschutzorganisation

DSFA-V "Datenschutz-Folgenabschätzung" VI

Folgenabschätzung verpflichtend (Beispiele aus Erläuterungen):

- Bildverarbeitungen an Örtlichkeiten denen man nicht "ausweichen" kann: Verkehrsbetriebe ("faktische Monopolstellung")
- Bildverarbeitungen in Spitäler, Ämter und Behörden sowie Polizeidienststellen, Mehrparteien-Wohnhäuser, Stätten der Religionsausübung
- Bodycams
- Kombination aus Fingerabdruck- und (biometrischer) Gesichtserkennung zur Zugangskontrolle
- gemeinsame Verarbeitung großer Datenmengen
- „Fraud-Prevention-Systeme“ und Scoringmethoden zur Verringerung (finanzieller) Ausfallsrisken
- Verarbeitungen im Zusammenhang mit Gesundheit, das Sexualleben und das Leben in und mit der Familie
- Verarbeitung besonderer Datenkategorien
- Verarbeitung von Standortdaten inklusive GPS
- Verarbeitung Daten von Kindern (bis 14 Jahre) und Asylbewerber
- Mitarbeiterdaten, sofern nicht bloß Personalverwaltung und keine BV existiert
- Verarbeitung Daten von Patienten, psychisch Kranke, sofern nicht bloß von einem einzelnen Arzt erfolgt und nicht unter die Ausnahme der DSFA-AV A12 fällt

VO SS2019 - Juridicum

DSFA-V - Entwurf:

Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Fortsetzung)

h) Kirchen, Gebetshäuser und andere Einrichtungen, die für die Religionsausübung genutzt werden, erfassen.

4. Verarbeitung von Daten unter Nutzung oder Anwendung neuer bzw. neuartiger Technologien oder organisatorischer Lösungen, welche die Abschätzung der Auswirkungen auf die Betroffenen und die gesellschaftlichen Folgen erschweren, insbesondere durch den Einsatz von künstlicher Intelligenz und die Verarbeitung biometrischer Daten, sofern die Verarbeitung nicht die bloße Echtzeitwiedergabe von Gesichtsbildern betrifft.

5. Verarbeitungsvorgänge von gemäß Art. 26 DSGVO gemeinsam für die Verarbeitung Verantwortlichen.

6. Zusammenführung und/oder Abgleich von Datensätzen aus zwei oder mehreren Verarbeitungen im Rahmen einer Datenverarbeitung, die zu unterschiedlichen Zwecken und/oder von verschiedenen Verantwortlichen durchgeführt wurden, die über die von einem Betroffenen üblicherweise zu erwartenden Verarbeitungen hinausgehen, sofern

a) diese für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt beim Betroffenen erhoben wurden, oder

b) durch die Anwendung von Algorithmen Entscheidungen getroffen werden können, welche die betroffenen Personen in erheblicher Weise beeinträchtigen.

7. Verarbeitungsvorgänge im höchstpersönlichen Bereich von Personen, auch wenn die Verarbeitung auf einer Einwilligung beruht.

Im Zusammenhang mit Beschäftigungsverhältnissen gilt dies nicht, wenn eine Betriebsvereinbarung oder Zustimmung der Personalvertretung vorliegt. Als systematische Überwachung sind jene Vorgänge zu verstehen, die im Rahmen eines Systems oder vorab festgelegt, organisiert und methodisch erfolgen.

(3) Eine Datenschutz-Folgenabschätzung ist durch den Verantwortlichen durchzuführen, wenn ein Verarbeitungsvorgang zwei oder mehr der nachstehenden Kriterien erfüllt:

1. Verarbeitung von besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO,

2. Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO,

3. Erfassung von Standortdaten im Sinne des § 92 Abs. 3 Z 6 Telekommunikationsgesetz 2003 – TKG 2003, BGBl. I. Nr. 70/2003, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben, oder

4. die Verarbeitung von Daten zu schutzbedürftigen Betroffenen, wie unmündigen Minderjährigen, Arbeitnehmern, Patienten, psychisch Kranken und Asylwerbern.

DSGVO - Datenschutzorganisation

DSGVO Art. 35 "Datenschutz-Folgenabschätzung" VII

Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 ist zu berücksichtigen (Abs. 8)

Datenschutzbeauftragter (falls vorhanden) MUSS konsultiert werden

Verantwortlicher holt Standpunkt der Betroffenen oder deren Vertreter ein (Abs. 9 " Mitwirkungs- und Mitspracherechte ")
[Anm: wird bei Mitarbeiterverarbeitungen Bedeutung erlangen]

Keine verpflichtende Folgenabschätzung (Abs. 10) bei gesetzlich angeordneten Verarbeitungen, sofern

+ Verarbeitung gemäß Art. 6 Abs. 1 lit c [zur Erfüllung einer rechtlichen Verpflichtung erforderlich] oder e [Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen]
+ konkreter Verarbeitungsvorgang oder konkrete Verarbeitungsvorgänge geregelt sind
+ Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte

VO SS2019 - Juridicum

DSGVO Art. 35 Datenschutz-Folgenabschätzung (Fortsetzung)

(8)Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9)Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10)Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11)Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Erforderlichkeit

Liegt eine Verpflichtung zur Folgenabschätzung vor?

- **neue Technologien**
  heuristische Verfahren, statistische Verfahren
  (zB biometrische Analysen, biometrische Identitätsfeststellung)
  Beobachten von Surf- oder Kaufverhalten
  automatisiertes Generieren von Empfehlungen
- **besonderer Umfang der Daten**
- **besondere Zwecke**
- **systematischer Einsatz von Profiling**
- **umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten**
- **umfangreiche Verarbeitung strafrechtlicher Verurteilungen und Straftaten**
- systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche: Videoüberwachung, Kundentracking im Kaufhaus, ...
- **sonstige Risiken**

VO SS2019 - Juridicum

-

DSGVO - Datenschutzorganisation

DPIA Beispiele - Internetanwendungen

- ☐ Parkplatz-Suchsystem
- ☐ Online-Authentifizierung (zB Video-Identifikation)
- ☐ Online-Kreditantragsbearbeitung
- ☐ Smart-TV
- ☐ Sprachassistenten
- ☐ Routen-Planer
- ☐ Kreditscoring
- ☐ Matching-Algorithmen
- ☐ Bewertungsplattformen
- ☐ Benutzer-Tracking
- ☐ Partnerbörse
- ☐ ...

VO SS2019 - Juridicum

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Verarbeitungsschritte (Analyse der Detailprozesse)

- **Datenerfassung** (Online-Formular, Papier-Formular, interne Eingabemaske, ...)
- **Datenkorrektur** (Antrag schriftlich, mündlich, telefonisch, interne Korrektur)
- **Berechnungsverfahren** (Scoringwert, Profiling, Vergleichs- oder Grenzwerte)
- **Auswertung** (Datenzuordnung, ...)
- **Übermittlung an Dritte**
- **Veröffentlichung** (Freigabe von Daten, ...)
- **Ausdrucke** (zB Reports, Berichte, Etikettierung bei Medizinprodukten, ...)
- **Backup- und Restore** (Backup funktioniert nicht, Medium defekt, falsche/veraltete Daten werden restored, ..)
- **Löschen von Daten** (unbeabsichtigtes Löschen, Löschen falsche Daten, ...)
- **Datenzugriff** (erwünscht/unerwünscht intern, durch Dritte, Malware, Hacking, ...)
- **???**

VO SS2019 - Juridicum

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Schäden

Welche potentiellen Schäden können identifiziert werden?
Hinweise gibt EW 75, 85 der DSGVO

Schäden durch fehlerhafte Datenverarbeitungen:

- physischem, materiellem oder imateriellem Schaden
- Diskriminierung
- Identitätsdiebstahl oder -betrug
- finanziellem Verlust
- Rufschädigung
- Verlust der Vertraulichkeit von einem dem Berufsgeheimnis unterliegende Daten
- wirtschaftlichem oder gesellschaftlichem Nachteil
- Verlust von Rechten und Freiheiten
- Kontrollverlust über die eigenen Daten
- falscher Bewertung der Person (zB im Zusammenhang mit Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlichen Vorlieben oder Interessen, Zuverlässigkeit, sonstigem Verhalten, ...)

VO SS2019 - Juridicum

DSGVO EW75

(75) Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Schadensklassen

Schäden werden in Schadensklassen gegliedert

Empfohlen wird gerade Zahl von Schadensklassen und wenige Klassen (4-6)

- **Finanzielle Schadensklassen:**
  [SA] < 100,- EUR
  [SB] 100 bis 1.000,- EUR
  [SC] 1.000 bis 100.000 EUR
  [SD] > 100.000 EUR
  (absolute Höhen werden vom Betroffenenkreis abhängen)
- **Schadensklassen Reputation:**
  [SA] geringe Personenanzahl, Person wird nicht eindeutig identifiziert
  [SB] unmittelbares Umfeld
  (zB engerer Familienkreis, Abteilungskollegen, <20 Personen)
  [SC] beschränktes Umfeld *(zB Hausgemeinschaft, Unternehmen, Kunden, Lieferanten, 20-200 Personen)*
  [SD] unbeschränktes Umfeld *(zB Medien, Online, ...)*

VO SS2019 - Juridicum

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Schadensklassen II

- **Schadensklassen Fehltherapie**
  [SA] überflüssige Behandlungsmaßnahmen sind faktisch ausgeschlossen
  [SB] geringfügige zusätzliche überflüssige Behandlungsmaßnahmen *(zB Medikamentation die grundsätzlich geeignet ist)*
  [SC] belastende zusätzliche überflüssige Behandlungsmaßnahmen *(zB Medikamentation die nicht geeignet ist mit geringen Nebenwirkungen)*
  [SD] erhebliche Belastung durch überflüssige Maßnahmen *(zB Medikation die zusätzliche Therapien auslöst)*
- **Schadensklassen medizinische Behandlungsfehler**
  [SA] Maßnahmen die auch Nichtmediziner erkennen und korrigieren kann *(zB fehlerhafter Verband)*
  [SB] leicht korrigierbare Maßnahmen *(zB geringfügig fehlerhafte Dosierung)*
  [SC] korrigierbare Maßnahmen *(zB falsche Implantate)*
  [SD] nicht korrigierbare Maßnahmen *(zB Amputationen)*

VO SS2019 - Juridicum

-

Datenschutz-Folgenabschätzung - Schadensklassen III

- **Schadensklassen Beratungs- und Betreuungfehler**
  [SA] Fehlende Vertragsunterlagen, die nachgereicht werden können
  [SB] Abschluss eines nicht erwünschten, aber grundsätzlich geeigneten Vertrages
  [SC] Abschluss eines ungeeigneten Vertrages
  [SD] Abschluss eines falschen Vertrages
- **Schadensklassen Zeitverlust**
  [SA] < 1 Stunde
  [SB] 1 bis 10 Stunden
  [SC] 1 bis 120 Stunden
  [SD] > 120 Stunden

-

Datenschutz-Folgenabschätzung - Eintrittshäufigkeit

- **Wahrscheinlichkeit des Eintritts**
  - **[H1]** < 1 mal pro Jahr
  - **[H2]** < 1 mal pro Monat
  - **[H3]** < 1 mal pro Woche
  - **[H4]** > 1 mal pro Woche

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Risikomatrix

Häufigkeit				
H4: > 1 mal pro Woche	SA / H4	SB / H4	SC / H4	SD / H4
H3: < 1 mal pro Woche	SA / H3	SB / H3	SC / H3	SD / H3
H2: 1 - 12 mal jährlich	SA / H2	SB / H2	SC / H2	SD / H2
H1: < 1 mal pro Jahr	SA / H1	SB / H1	SC / H1	SD / H1
	SA: Partner erfährt von Vorfall	SB: Bekannte erfahren von Vorfall	SC: Arbeit-geber erfährt von Vorfall	SD: Öffentlichkeit, unbekannter Personenkreis	**Reputations-schaden**

➡ Maßnahmen MÜSSEN VOR Beginn der Verarbeitung gesetzt werden

➡ Maßnahmen SOLLTEN ergriffen werden, KANN im laufenden Betrieb erfolgen

VO SS2019 - Juridicum

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Fallbeispiel

- **Verarbeitung:** Kontoführung
- **Verarbeitungsschritt:** Mitteilungen an Betroffenen
- **Bedrohung iS Art. 35 Abs. 1:** Offenlegung Finanzdaten
- **Schwachstelle:** unzureichendes Kommunikationsmittel
- **Schadensklasse:** Reputation, finanzieller Schaden

Potentielle Bedrohung	Basis Eintrittshäufigkeit und Schadenshöhe je Ereignis	getroffene Maßnahmen	Behandlung Restrisiko
Mögliche Schwachstelle	**Bewertung Basisrisiko** (erfolgt auf Basis bisheriger Erfahrungen, ist regelmäßig zu evaluieren)	**Bewertung Restrisiko**	
Eine Bank informiert seine Kunden per eMail über ausstehende Kreditraten. Die Kunden haben dem Versand zugestimmt.	In einem von 100 Fällen wird das eMail auf Grund der Autovervollständigung an eine Person ähnlichen Namens verschickt. Die Bank bearbeitet am Tag mehr als 2000 Fälle.	Die Funktion Autovervollständigung wird deaktiviert. Es kommt nur mehr zu Fehlzustellungen in 1 von 10.000 Fällen.	(a) eMails werden nur mit Schlüssel des berechtigten Empfängers verschickt (b) die eMailsenthalten keine Kreditdaten, sondern nur eine Auffoderung mit der Bank in Kontakt zu treten (c) auf eMail-Kommunikation wird verzichtet
Verwendet wird Outlook ohne Verschlüsselung und "Autovervollständigung" der eMail-Adresse	**SD / H4**	**SD / H4**	

VO SS2019 - Juridicum

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Fallbeispiel

- **Verarbeitung:** dynamische KFZ-Versicherung
- **Verarbeitungsschritt:** Prämienberechung
- **Bedrohung iS Art. 35 Abs. 1:** automatisiertes Verfahren
- **Schwachstelle:** unzureichende Beachtung aller Einflussfaktoren
- **Schadensklasse:** finanzieller Schaden

Potentielle Bedrohung	Basis Eintrittshäufigkeit und Schadenshöhe je Ereignis	getroffene Maßnahmen	Behandlung Restrisiko
Mögliche Schwachstelle	**Bewertung Basisrisiko** (erfolgt auf Basis bisheriger Erfahrungen, ist regelmäßig zu evaluieren)	**Bewertung Restrisiko**	
KFZ-Inhaber erhalten Prämienrabatte, wenn sie durch ihr Fahrverhalten bestimmte Punktewerte erreichen. Der Rabatt beträgt zwischen 50 und 1.000 Euro.	In 10 von 100 Fällen erfolgt keine Prämiengutschrift, obwohl bei objektiver Analyse des Fahrverhaltens alle Vorgaben der Straßenverkehrsordnung eingehalten werden. 50.000 Personen nutzen diese Versicherungsform.	Es wird ein Algorithmus eingesetzt, der von unabhängigen Sachverständigen zertifiziert ist. Die mögliche Rabatthöhe wird reduziert.	Versicherungsnehmer werden über die Fehlerhaftigkeit ausführlich informiert. Die Einspruchsrechte der Betroffenen werden ausgeweitet. Der Algorithmus wird laufend korrigiert.
Unzureichender Berechnungsalgorithmus, fehlerhafte Datenermittlung	**SC / H4**	**SA / H3**	

VO SS2019 - Juridicum

-

DSGVO - Datenschutzorganisation

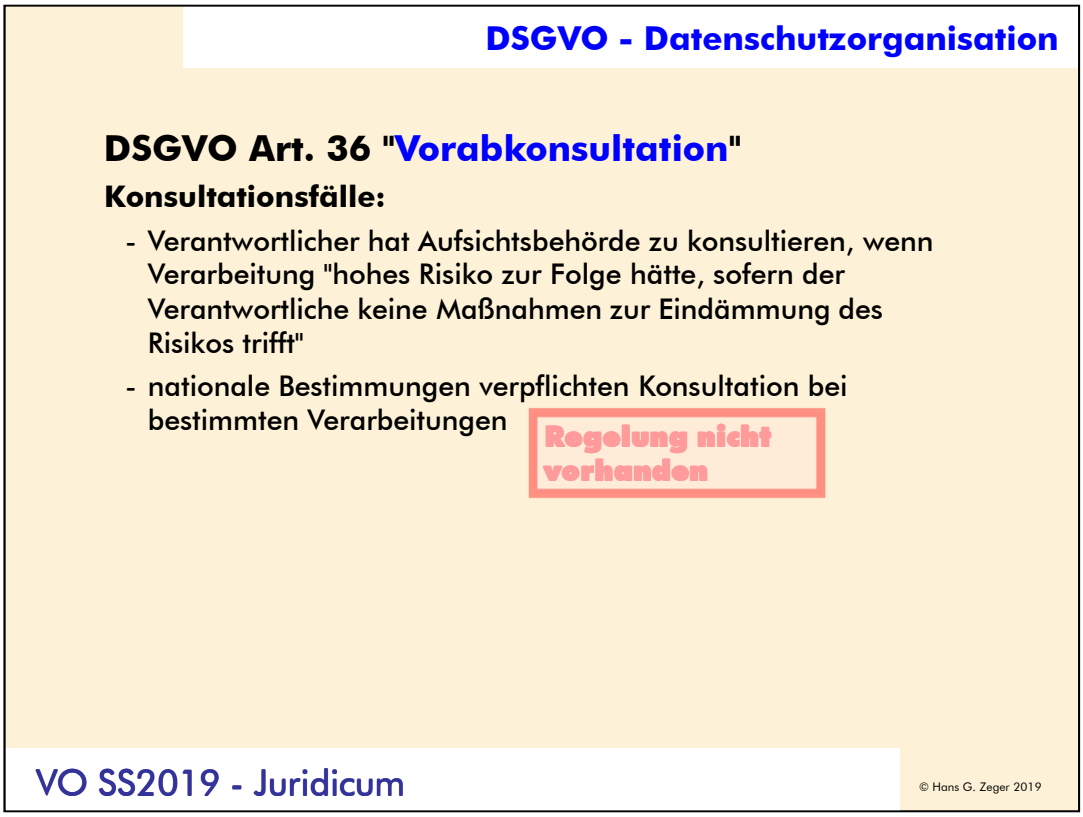
Datenschutz-Folgenabschätzung - Fallbeispiel

- **Verarbeitung:** Kreditvergabe
- **Verarbeitungsschritt:** Online-Kreditantrag
- **Bedrohung iS Art. 35 Abs. 1:** Profiling (hier: Geoscoring)
- **Schwachstelle:** Fehlerhafte/unvollständige Datenerfassung
- **Schadensklasse:** Mehrkosten Kredit / Kreditablehnung

Potentielle Bedrohung	Basis Eintrittshäufigkeit und Schadenshöhe je Ereignis	getroffene Maßnahmen	Behandlung Restrisiko
Mögliche Schwachstelle	**Bewertung Basisrisiko** (erfolgt auf Basis bisheriger Erfahrungen, ist regelmäßig zu evaluieren)	**Bewertung Restrisiko**	
Es erfolgt auf Basis der Onlineangaben des Betroffenen im Hintergrund ein Geoscoring	mehr als einmal pro Woche, kann zu Kreditablehnung führen und dem Betroffenen Mehrkosten > 1.000,- Euro verursachen	Genaue Aufklärung, dass geoscoring gemacht wird und daher Kreditkonditionen nur mit korrekter Adresse richtig berechnet werden können	Vor Berechnung der Kreditkonditionen wird das vorliegende Scoringergebnis auch inhaltlich geprüft.
Antragsteller gibt jedoch unvollständige Adressdaten bekannt	**SC / H4**	**SA / H2**	

VO SS2019 - Juridicum

-



DSGVO Art. 36 Vorherige Konsultation

(1)Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

(2)Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 1 nicht im Einklang mit dieser Verordnung stünde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu acht Wochen nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen und kann ihre in Artikel 58 genannten Befugnisse ausüben. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um sechs Wochen verlängert werden. Die Aufsichtsbehörde unterrichtet den Verantwortlichen oder gegebenenfalls den Auftragsverarbeiter über eine solche Fristverlängerung innerhalb eines Monats nach Eingang des Antrags auf Konsultation zusammen mit den Gründen für die Verzögerung. Diese Fristen können ausgesetzt werden, bis die Aufsichtsbehörde die für die Zwecke der Konsultation angeforderten Informationen erhalten hat.

(3)Der Verantwortliche stellt der Aufsichtsbehörde bei einer Konsultation gemäß Absatz 1 folgende Informationen zur Verfügung:

a) gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;

b) die Zwecke und die Mittel der beabsichtigten Verarbeitung;

c) die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;

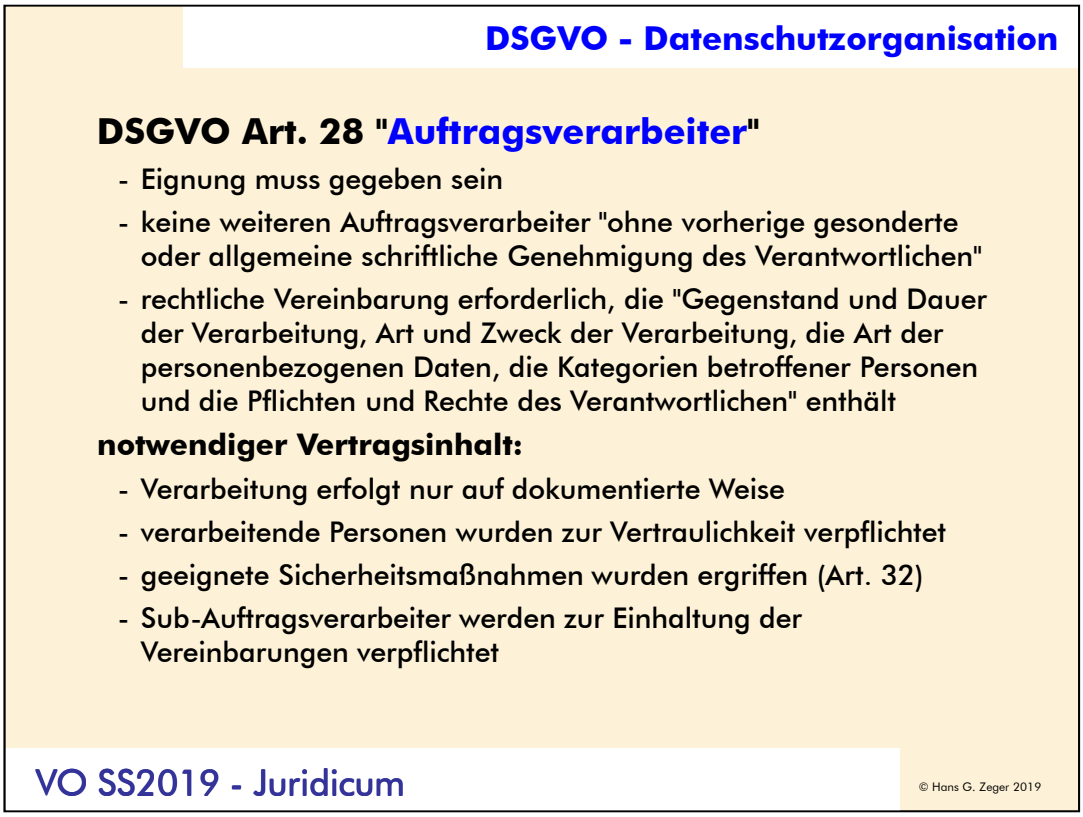
d) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

e) die Datenschutz-Folgenabschätzung gemäß Artikel 35 und

f) alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

(4)Die Mitgliedstaaten konsultieren die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung betreffen.

(5)Ungeachtet des Absatzes 1 können Verantwortliche durch das Recht der Mitgliedstaaten verpflichtet werden, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen.



DSGVO Art. 28 Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

DSGVO - Datenschutzorganisation

DSGVO Art. 28 "Auftragsverarbeiter" II

notwendiger Vertragsinhalt (Fortsetzung):

- Unterstützung des Verantwortlichen zur Einhaltung der Betroffenenrechte und sonstiger Verpflichtungen gemäß DSGVO
- nach Abschluss der Verarbeitung löscht Auftragsverarbeiter alle Daten oder gibt sie zurück (sofern dem nicht gesetzliche Regelungen entgegen stehen)
- stellt dem Verantwortlichen alle notwendigen Informationen zur Einhaltung seiner Verpflichtungen bereit und ermöglicht gegebenenfalls auch Inspektionen

Vertragsgestaltung:

- kann ein Standardvertrag der EU-Kommission verwendet werden
- Vertrag ist schriftlich abzufassen (elektronische Form ist zulässig)

VO SS2019 - Juridicum

DSGVO Art. 28 Auftragsverarbeiter (Fortsetzung)

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d)die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e)angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

DSGVO - Datenschutzorganisation

DSGVO Art. 28 "Auftragsverarbeiter" III

Nachweis der Eignung:

- Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder
- Einhaltung eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter

kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

Auftragsverarbeiter wird Verantwortlicher, wenn er persönliche Daten entgegen den Bestimmungen der DSGVO verwendet

VO SS2019 - Juridicum

DSGVO Art. 28 Auftragsverarbeiter (Fortsetzung)

(4)Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind,

(5)Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6)Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7)Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8)Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9)Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10)Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

IT-Sicherheit, DSGVO und Cloud-Computing

Was ist Cloud-Computing?

- **technisch: Nutzung fremder IT-Infrastruktur in verschiedenen Ausformungen: IaaS, PaaS, SaaS, public, private oder hybride Cloud**
- **im Lichte des DSGVO:** nur relevant, wenn Daten Dritter ("Betroffener") verarbeitet werden, Auftragsverarbeitung im Sinne DSGVO Art. 28 mit Verpflichtung Sicherheitsmaßnahmen iS DSGVO Art. 32 einzuhalten

Verantwortlicher bleibt verantwortlich, egal wie die Cloud-Lösung organisiert ist, auch bei Heranziehung von Sub- und Sub-Sub-Auftragsverarbeitern

VO SS2019 - Juridicum

- PaaS: Platform as a Service
- SaaS: Software as a Service
- IaaS: Infrastructure as a Service

IT-Sicherheit, DSGVO und Cloud-Computing

Basisfragen, die bei Cloudeinsatz gelöst sein müssen

- **verantwortlich für den Einsatz von Daten ist der Verantwortliche** (Art. 4 Z 7 DSGVO)
- **den Verantwortlicher trifft Verpflichtung geeigneten Auftragsverarbeiter auszuwählen inkl. aller Sub-Auftragsverarbeiter** (Art. 28 Abs. 1 DSGVO)
- **der Verantwortlicher hat schriftlich geeignete Vereinbarungen abzuschließen** (Art. 28 Abs. 3 DSGVO)
- **der Verantwortlicher hat die Tätigkeit der Auftragsverarbeiter zu überwachen** (Art. 28 Abs. 3 lit h DSGVO)
- **der Verantwortlicher kann die Beiziehung von Sub-Auftragsverarbeitern verbieten** (Art. 28 Abs. 2 DSGVO)

VO SS2019 - Juridicum

-

IT-Sicherheit, DSGVO und Cloud-Computing

Basisfragen, die bei Cloudeinsatz gelöst sein müssen II

- der Verantwortlicher hat für Umsetzung der richtigen sicherheitstechnischen Maßnahmen gemäß DSGVO Art. 32 zu sorgen (Art. 28 Abs. 3 lit c DSGVO)
- bei Nachweis der Einhaltung genehmigter Verhaltensregeln gemäß DSGVO Art. 40 oder genehmigter Zertifizierungsverfahren gemäß DSGVO Art. 42 durch Auftragsverarbeiter gilt die Vermutung der Erfüllung der Sicherheitsmaßnahmen (Art. 32 Abs. 3 DSGVO)

Die Cloudfragen sind durch eine geeignete Kombination technischer und organisatorischer (vertraglicher) Maßnahmen zu lösen!

VO SS2019 - Juridicum

-

DSGVO - Datenschutzorganisation

DSGVO Art. 37
"Benennung Datenschutzbeauftragter"

(gilt für Verantwortliche und Auftragsverarbeiter)

verpflichtende Benennung:

- Verarbeitung durch Behörde oder öffentliche Stelle, mit Ausnahme von Gerichten, im Rahmen ihrer justiziellen Tätigkeit
  [Anm: keine inhaltlichen oder personellen Ausnahmen!]
- Kerntätigkeit ist eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen
  [Anm: ??? Informationsdienste, Detektive, Sicherheitsdienste, ...]
- Kerntätigkeit ist die umfangreiche Verarbeitung besonderer Kategorien von Daten [Anm: Spitäler JA, Ärzte NEIN]
- Kerntätigkeit ist die umfangreiche Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten
- nationale Bestimmungen verpflichten zu Datenschutzbeauftragten [in Österreich nicht umgesetzt]

VO SS2019 - Juridicum

DSGVO Art. 37 Benennung eines Datenschutzbeauftragten

(1)Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,

b)die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

(2)Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.

(3)Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.

DSGVO - Datenschutzorganisation

DSGVO Art. 37
"Benennung Datenschutzbeauftragter" II

Organisationsbestimmungen:

- Unternehmensgruppe darf gemeinsamen Datenschutzbeauftragten ernennen
- Behörde oder öffentliche Stelle, kann für mehrere vergleichbare Behörden oder Stellen gemeinsamen Datenschutzbeauftragten ernennen
- Verbände und andere Vereinigungen können Datenschutzbeauftragten ernennen, der in Vertretung der Verantwortlichen handeln kann ["Kammer-Datenschutz-Beauftragter"]
- interner oder externer Datenschutzbeauftragter ist zulässig
- Kontaktdaten des Datenschutzbeauftragten sind Aufsichtsbehörde mitzuteilen und zu veröffentlichen

VO SS2019 - Juridicum

DSGVO Art. 37 Benennung eines Datenschutzbeauftragten (Fortsetzung)

(4)In anderen als den in Absatz 1 genannten Fällen können der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen. Der Datenschutzbeauftragte kann für derartige Verbände und andere Vereinigungen, die Verantwortliche oder Auftragsverarbeiter vertreten, handeln.

(5)Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.

(6)Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(7)Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

DSGVO - Datenschutzorganisation

DSGVO Art. 38
"Stellung Datenschutzbeauftragter"

- frühzeitige Einbindung in Verarbeitungsprojekte
- Bereitstellung erforderlicher Ressourcen
- Ermöglichen des Zugangs zu den personenbezogenen Daten und Verarbeitungsvorgängen
- Weisungsfrei bezüglich der Ausübung dieser Aufgaben
- Keine Abberufung im Zusammenhang mit seiner Tätigkeit
- Datenschutzbeauftragter berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters
- Betroffene können sich in ALLEN Datenschutzfragen an Datenschutzbeauftragten wenden
- Datenschutzbeauftragter ist zur Vertraulichkeit verpflichtet
- andere Tätigkeiten zulässig, dürfen aber nicht in Konflikt stehen

VO SS2019 - Juridicum

DSGVO Art. 38 Stellung des Datenschutzbeauftragten

(1)Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2)Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen.

(3)Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.

(4)Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.

(5)Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.

(6)Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

DSGVO - Datenschutzorganisation

DSGVO Art. 39
"Aufgaben Datenschutzbeauftragter"

- Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen zu Dokumentationspflichten
- Überwachung der Umsetzung und Anwendung der Datenschutzstrategien
- Zuweisung von Zuständigkeiten
- Schulung der an den Verarbeitungen beteiligten Mitarbeiter
- Überwachung der Umsetzung und Anwendung der Grundverordnung Datenschutz, insbesondere an technische Datenschutz-Anforderungen, datenschutzfreundliche Voreinstellungen, an Datensicherheit, an Benachrichtigung betroffener Personen

VO SS2019 - Juridicum

DSGVO Art. 39 Aufgaben des Datenschutzbeauftragten

(1) Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

c) Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;

d) Zusammenarbeit mit der Aufsichtsbehörde;

e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

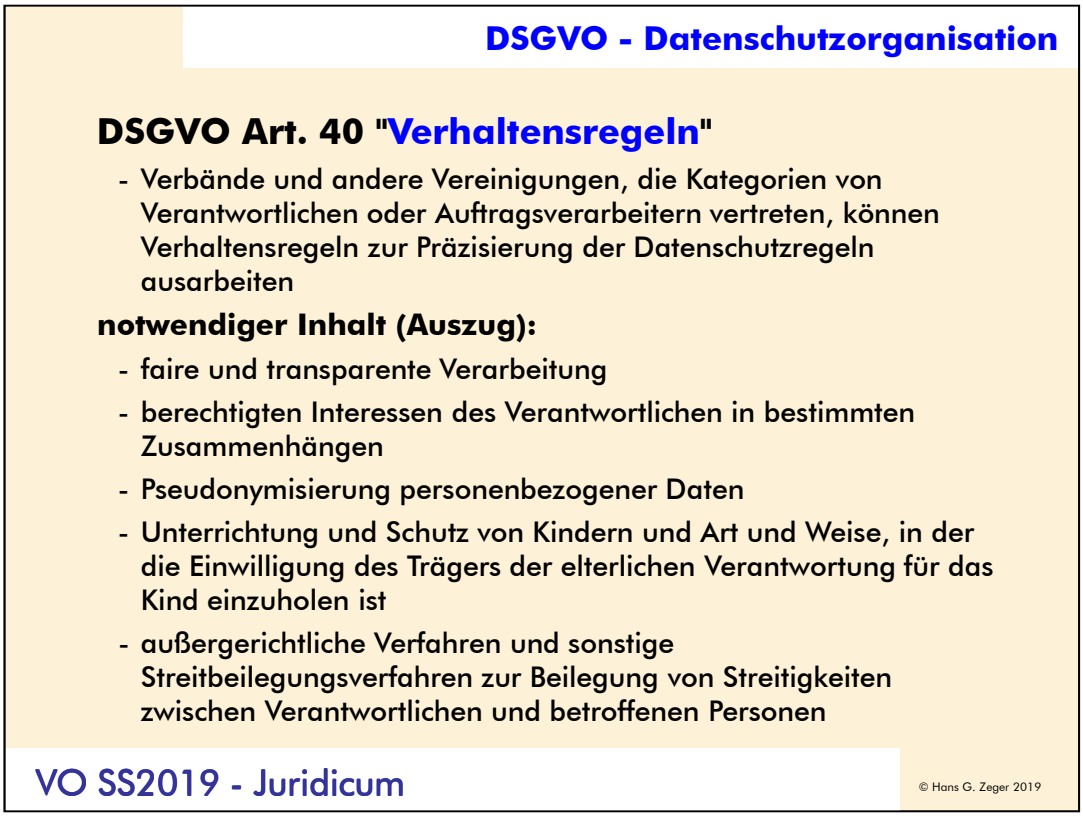
DSGVO - Datenschutzorganisation

DSGVO Art. 39
"Aufgaben Datenschutzbeauftragter" II

- Sicherung der Betroffenenrechte
- Sicherung und Überwachung aller erforderlichen Dokumentationen
- Meldung und Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten
- Überwachung der durchgeführten Datenschutz-Folgenabschätzung sowie Beantragung erforderlicher vorheriger Genehmigungen
- Überwachung der durch die Aufsichtsbehörde angeordneten Maßnahmen
- Ansprechpartner und Zusammenarbeit mit der Aufsichtsbehörde

VO SS2019 - Juridicum

-



DSGVO Art. 40 Verhaltensregeln

(1)Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen.

(2)Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können Verhaltensregeln ausarbeiten oder ändern oder erweitern, mit denen die Anwendung dieser Verordnung beispielsweise zu dem Folgenden präzisiert wird:

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 Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 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 Artikeln 77 und 79.

DSGVO Art. 44 Allgemeine Grundsätze der Datenübermittlung

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

DSGVO Art. 45 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1)Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

(2)Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus berücksichtigt die Kommission insbesondere das Folgende:

a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art — auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten — sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,

b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

DSGVO Art. 45 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses (Fortsetzung)

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels bieten. In dem Durchführungsrechtsakt ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b des vorliegenden Artikels genannte Aufsichtsbehörde bzw. genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und bei internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 des vorliegenden Artikels erlassenen Beschlüsse und der nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen beeinträchtigen könnten.

(5) Die Kommission widerruft, ändert oder setzt die in Absatz 3 des vorliegenden Artikels genannten Beschlüsse im Wege von Durchführungsrechtsakten aus, soweit dies nötig ist und ohne rückwirkende Kraft, soweit entsprechende Informationen — insbesondere im Anschluss an die in Absatz 3 des vorliegenden Artikels genannte Überprüfung — dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifischer Sektor in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels mehr gewährleistet. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen. In hinreichend begründeten Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 93 Absatz 3 genannten Verfahren sofort geltende Durchführungsrechtsakte.

(6) Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem gemäß Absatz 5 erlassenen Beschluss geführt hat.

(7) Übermittlungen personenbezogener Daten an das betreffende Drittland, das Gebiet oder einen oder mehrere spezifische Sektoren in diesem Drittland oder an die betreffende internationale Organisation gemäß den Artikeln 46 bis 49 werden durch einen Beschluss nach Absatz 5 des vorliegenden Artikels nicht berührt.

(8) Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Drittländer beziehungsweise Gebiete und spezifischen Sektoren in einem Drittland und aller internationalen Organisationen, für die sie durch Beschluss festgestellt hat, dass sie ein angemessenes Schutzniveau gewährleisten bzw. nicht mehr gewährleisten.*

(9) Von der Kommission auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie durch einen nach dem Prüfverfahren gemäß den Absätzen 3 oder 5 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

DSGVO - Internationaler Datenverkehr

Genehmigungsfrei (weil gleichwertig)

- **gleichwertig auf Grund EWR-Verträge**
  Island, Norwegen, Liechtenstein
- **gleichwertig gem. Kommissionsentscheidung**
  Schweiz (27.7.2000), Kanada (15.1.2002), Argentinien (30.6.2003), Israel (31.1.2011), Uruguay (23.8.2012), Neuseeland (30.1.2013)
  + Andorra, Färöer Islands, Guernsey, Isle of Man, Jersey
- **USA** (nur bereichs- oder unternehmensbezogen, wenn PrivacyShield-Vereinbarung beigetreten, eigene SWIFT- oder PassengerNameRecord-Abkommen)

- bisherige Gleichwertigkeitsentscheidungen wurden übernommen
- **gleichwertig seit 25.5.2018**: Japan (23.1.2019)
- **in Verhandlung**: Südkorea

bei allen anderen Staaten hat sich der Betroffene bzw. der Verantwortlicher um den Datenschutz zu kümmern

VO SS2019 - Juridicum

Aktueller Stand der gleichwertigen Länder:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_de
(STAND: 3/2019)

Suchbegriffe: "Commission decisions adequacy protection personal data third countries" auf http://ec.europa.eu/

EG-Standardvertragsklauseln:

Version 1 (2001):
ftp://ftp.freenet.at/privacy/ds-eu/eg-standardvertragsklauseln-1.pdf

Version 2 (2004):
ftp://ftp.freenet.at/privacy/eu-ds/eu-standardvertragsklauseln-2.pdf

Wichtige Vertragselemente der Standardvertragsklauseln

Auswahlhaftung des Datenexporteurs: muss sich von der Fähigkeit des Importeurs bei der Einhaltung der Datenschutzbestimmungen überzeugen

bei Datenschutzverletzungen: zuständig ist das Gericht, in dem Land in dem der Datenexporteur seinen Sitz hat

Durchsetzungfrist bei Datenschutzrechten: ein Monat

DSGVO - Internationaler Datenverkehr

Was bedeutet "Privacy Shield"?

In den USA fehlen einheitliche, für Unternehmen verbindliche Datenschutzstandards

Entwicklung von Richtlinien, denen freiwillig beigetreten werden kann (SELBSTZERTIFIZIERUNG), nach Beitritt verbindlich

FTC (Federal Trade Commission, Bundeshandelskommission) bzw DOT (Department of Transportation bei Luftfahrtgesellschaften) überwachen Einhaltung

Liste mit Teilnehmern veröffentlicht, Stand Oktober 2016: ca. 320 Organisationen, etwa 10 % der früheren Safe Harbour-Liste, ua Facebook, Google, Microsoft

Beitritt betrifft "alle" persönlichen Daten, es kann jedoch für HR-Daten (Personaldaten) Ausnahme vorgesehen werden

VO SS2019 - Juridicum

Unterlagen zur Entscheidung der EU-Kommission "über die Angemessenheit des Datenschutzes in den USA":

http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

Pressemitteilung EU-Kommission "über die Angemessenheit des Datenschutzes in den USA":

http://europa.eu/rapid/press-release_IP-16-2461_en.htm

...

The EU-U.S. Privacy Shield is based on the following principles:

Strong obligations on companies handling data: under the new arrangement, the U.S. Department of Commerce will conduct **regular updates and reviews** of participating companies, to ensure that companies follow the rules they submitted themselves to. If companies do not comply in practice they face sanctions and removal from the list. The tightening of conditions for the **onward transfers** of data to third parties will guarantee the same level of protection in case of a transfer from a Privacy Shield company.

Clear safeguards and transparency obligations on U.S. government access: The **US has given the EU assurance** that the access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversight mechanisms. Everyone in the EU will, also for the first time, benefit from **redress mechanisms** in this area. The U.S. has ruled out indiscriminate mass surveillance on personal data transferred to the US under the EU-U.S. Privacy Shield arrangement. The Office of the Director of National Intelligence further clarified that bulk collection of data could only be used under specific preconditions and needs to be as targeted and focused as possible. It details the safeguards in place for the use of data under such exceptional circumstances. The U.S. Secretary of State has established a **redress possibility** in the area of national intelligence for Europeans through an **Ombudsperson mechanism** within the Department of State.

DSGVO - Internationaler Datenverkehr

zentrale Grundsätze des "Privacy Shield"

- Framework liest sich wie Kurzfassung der EU-Grundverordnung
- Definition von persönlichen Daten, Datenverarbeitung und Verantwortlichen durchaus mit EU-Niveau vergleichbar
- wichtige Elemente sind enthalten: Zweckbestimmung, Informationspflicht, Regelungen zur Datenweitergabe, Sicherheitsbestimmungen, Regeln zur Sicherung der Datenintegrität, Löschungs- und Auskunftsrechte
- sensible Daten ähnlich EU definiert
- Rechtsdurchsetzung grundsätzlich in USA, aber Unternehmen kann auch EU-Datenschutzaufsicht akzeptieren
- Datenweitergabe an Dritte bedürfen nur bei sensiblen Daten ausdrückliche Zustimmung (inkl. Ausnahmen), ansonsten eher Opt-Out
- bei Weitergabe an Dritte müssen diese NICHT in Privacy Shield Liste eingetragen sein

VO SS2019 - Juridicum

EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE (Auszüge)

I. OVERVIEW

...

6. Organizations are obligated to **apply the Principles to all personal data transferred in reliance on the Privacy Shield after they enter the Privacy Shield**. An organization that chooses to extend Privacy Shield benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department and conform to the requirements set forth in the Supplemental Principle on Self-Certification.

7. **U.S. law will apply** to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with European data protection authorities ("DPAs"). Unless otherwise stated, all provisions of the Principles apply where they are relevant.

8. Definitions:

a. **"Personal data"** and **"personal information"** are **data about an identified or identifiable individual** that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form.

b. **"Processing"** of personal data means **any operation or set of operations which is performed upon personal data, whether or not by automated means**, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

c. **"Controller"** means a person or organization which, alone or jointly with others, **determines the purposes and means of the processing of personal data**.

DSGVO - Internationaler Datenverkehr

DSGVO Art. 47 "Binding Corporate Rules (BCR)"

Rechtlich bindende Datenschutzregeln für eine Unternehmensgruppe (Abs. 1)

Notwendiger Inhalt (Abs. 2)

(a) Unternehmensstruktur, Kontaktdaten der Unternehmensgruppe und aller ihrer Mitglieder
(b) vollständige Information über die betroffenen Datenübermittlungen (inkl. Art der Daten, Zweck, betroffene Personengruppen)
(c) interne und externe Rechtsverbindlichkeit der betreffenden internen Datenschutzvorschriften
(d) Beschreibung der Anwendung der allgemeinen Datenschutzgrundsätze, der Sicherheitsmaßnahmen
(e) Beschreibung der Betroffenenrechte inkl. im Falle der Verletzung der verbindlichen internen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz
(f) Haftung der in den Mitgliedsstaaten niedergelassenen verantwortlichen

VO SS2019 - Juridicum

DSGVO Art. 47 Verbindliche interne Datenschutzvorschriften

(1)Die zuständige Aufsichtsbehörde genehmigt gemäß dem Kohärenzverfahren nach Artikel 63 verbindliche interne Datenschutzvorschriften, sofern diese

a) rechtlich bindend sind, für alle betreffenden Mitglieder der Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gelten und von diesen Mitgliedern durchgesetzt werden, und dies auch für ihre Beschäftigten gilt,

b) den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen und c) die in Absatz 2 festgelegten Anforderungen erfüllen.

(2)Die verbindlichen internen Datenschutzvorschriften nach Absatz 1 enthalten mindestens folgende Angaben:

a) Struktur und Kontaktdaten der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und jedes ihrer Mitglieder;

b) die betreffenden Datenübermittlungen oder Reihen von Datenübermittlungen einschließlich der betreffenden Arten personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;

c) interne und externe Rechtsverbindlichkeit der betreffenden internen Datenschutzvorschriften;

d) die Anwendung der allgemeinen Datenschutzgrundsätze, insbesondere Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rechtsgrundlage für die Verarbeitung, Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und Anforderungen für die Weiterübermittlung an nicht an diese internen Datenschutzvorschriften gebundene Stellen;

e) die Rechte der betroffenen Personen in Bezug auf die Verarbeitung und die diesen offenstehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung nach Artikel 22 unterworfen zu werden sowie des in Artikel 79 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen internen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;

f) die von dem in einem Mitgliedstaat niedergelassenen Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße eines nicht in der Union niedergelassenen betreffenden Mitglieds der Unternehmensgruppe gegen die verbindlichen internen Datenschutzvorschriften; der Verantwortliche oder der Auftragsverarbeiter ist nur dann teilweise oder vollständig von dieser Haftung befreit, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;

DSGVO - Internationaler Datenverkehr

DSGVO Art. 47 "Binding Corporate Rules (BCR)" II

Notwendiger Inhalt (Abs. 2) Fortsetzung

(g) Informationsverfahren der Betroffenen über die "Binding Corporate Rules"
(h) Aufgaben der Datenschutzbeauftragten
(i) Ablauf eines Beschwerdeverfahrens
(j) Beschreibung der Verfahren innerhalb der Unternehmensgruppe zur Einhaltung der BCR
(k) Verfahren zur Änderung und Meldung der Änderung der BCR bei den Aufsichtsbehörden
(l) Verfahren zur Zusammenarbeit mit den Aufsichtsbehörden
(m) Meldeverfahren über Änderungen von rechtlichen Bestimmungen in Drittländern die sich nachteilig auf den Datenschutz auswirken können
(n) geeignete Datenschutzschulungen der Mitarbeiter

VO SS2019 - Juridicum

DSGVO Art. 47 Verbindliche interne Datenschutzvorschriften (Fortsetzung)

g) die Art und Weise, wie die betroffenen Personen über die Bestimmungen der Artikel 13 und 14 hinaus über die verbindlichen internen Datenschutzvorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;

h) die Aufgaben jedes gemäß Artikel 37 benannten Datenschutzbeauftragten oder jeder anderen Person oder Einrichtung, die mit der Überwachung der Einhaltung der verbindlichen internen Datenschutzvorschriften in der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sowie mit der Überwachung der Schulungsmaßnahmen und dem Umgang mit Beschwerden befasst ist;

i) die Beschwerdeverfahren;

j) die innerhalb der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen internen Datenschutzvorschriften. Derartige Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Abhilfemaßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse derartiger Überprüfungen sollten der in Buchstabe h genannten Person oder Einrichtung sowie dem Verwaltungsrat des herrschenden Unternehmens einer Unternehmensgruppe oder der Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, mitgeteilt werden und sollten der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden;

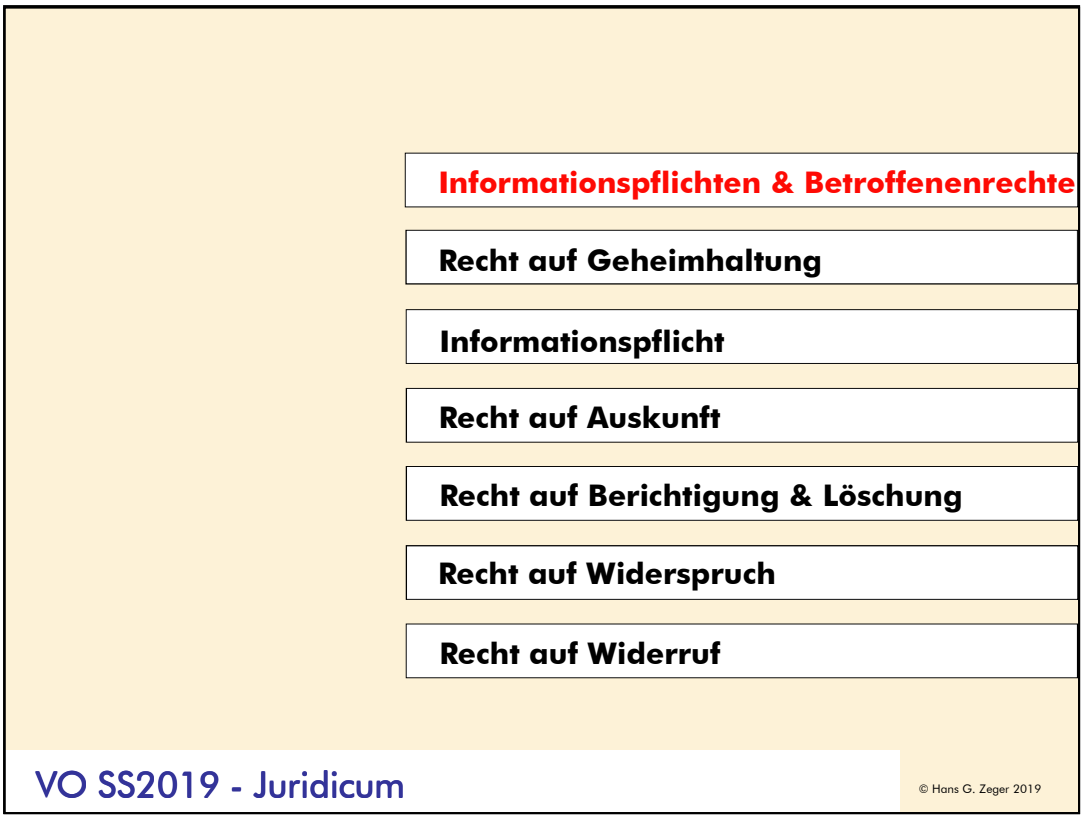
k) die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;

l) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gewährleisten, insbesondere durch Offenlegung der Ergebnisse von Überprüfungen der unter Buchstabe j genannten Maßnahmen gegenüber der Aufsichtsbehörde;

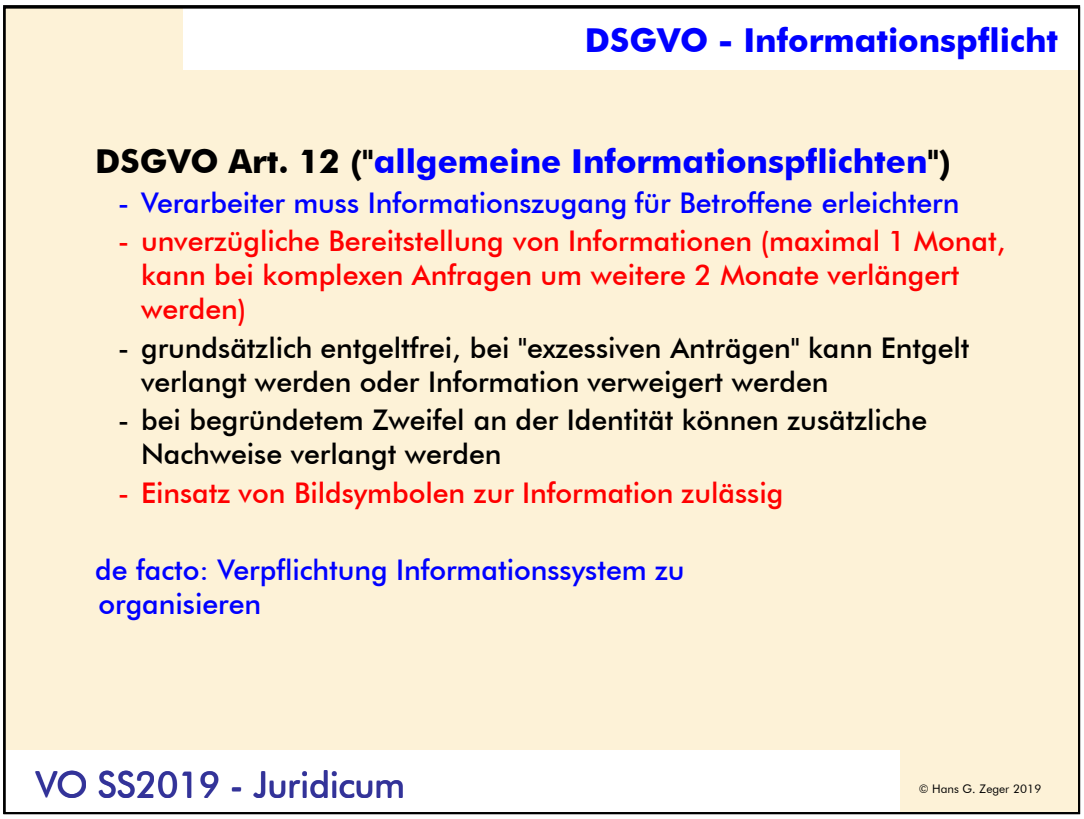
m)die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken könnten, die die verbindlichen internen Datenschutzvorschriften bieten, und

n) geeignete Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten.

(3)Die Kommission kann das Format und die Verfahren für den Informationsaustausch über verbindliche interne Datenschutzvorschriften im Sinne des vorliegenden Artikels zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden festlegen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.


Informationspflichten & Betroffenenrechte
Recht auf Geheimhaltung
Informationspflicht
Recht auf Auskunft
Recht auf Berichtigung & Löschung
Recht auf Widerspruch
Recht auf Widerruf
VO SS2019 - Juridicum
© Hans G. Zeger 2019

-



DSGVO Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1)Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

(2)Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22. In den in Artikel 11 Absatz 2 genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

(3)Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(4)Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5)Informationen gemäß den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(6)Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er unbeschadet des Artikels 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

(7)Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, müssen sie maschinenlesbar sein.

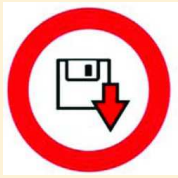
(8)Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen.

DSGVO - Informationspflicht

DSGVO Art. 13
"Informationspflicht Ermittlung bei Betroffenen"

Informationsumfang (soweit zutreffend)

- Name + Kontaktdaten des Verantwortlichen (inkl. Vertreter bzw. Datenschutzbeauftragten)
- Zwecke und Rechtsgrundlagen
- Empfänger oder Kategorien von Empfängern
- Informationen über Absicht die Daten an Drittländer ohne angemessenes Schutzniveau zu übermitteln
- Dauer der Datenspeicherung oder Kriterien die die Dauer bestimmen
- Gründe der Verarbeitung (im Fall der überwiegenden Interessen iS Art. 6 Abs. 1 lit f)
- Hinweis auf Betroffenenrechte (Auskunft, Berichtigung, Löschung, ...)



VO SS2019 - Juridicum

DSGVO Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1)Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden; e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2)Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

DSGVO - Informationspflicht

DSGVO Art. 13 "Informationspflicht Ermittlung bei Betroffenen" II

Informationsumfang (soweit zutreffend)

- Hinweis auf Widerrufsrecht (bei Verarbeitungen nach Art. 6 Abs. 1 lit a oder Art. 9 Abs. 2 lit a)
- Hinweis auf Beschwerderecht bei Aufsichtsbehörde
- Verpflichtung (bzw. Freiwilligkeit) der Bereitstellung der Informationen durch Betroffenen + Hinweis auf Konsequenzen
- Hinweis auf Bestehen einer automatisierten Entscheidungsfindung bzw. eines Profiling + aussagekräftige Informationen zur Entscheidungslogik
- Zeitgerechte Information des Betroffenen, wenn Daten für andere Zwecke verwendet werden sollen

Bestimmungen finden keine Anwendung, wenn Betroffener diese Informationen schon hat

VO SS2019 - Juridicum

DSGVO Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Fortsetzung)

b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3)Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4)Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

DSGVO - Informationspflicht

DSGVO Art. 14 "Informationspflicht Ermittlung nicht bei Betroffenen"

Ergänzend zu Art. 13

- Datenquelle (auch wenn öffentlich recherchiert)
- Kategorien der Daten

Verständigungsfristen (alternativ)

- innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats (Anwendungsfall: Informationsdienste, ...)
- spätestens zum Zeitpunkt der ersten Mitteilung an Betroffenen (Anwendungsfall: Kommunikation mit Betroffenem)
- bei Offenlegung an einen anderen Empfänger, spätestens zum Zeitpunkt der ersten Offenlegung

VO SS2019 - Juridicum

DSGVO Art. 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1)Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) die Kategorien personenbezogener Daten, die verarbeitet werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.

(2)Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird; e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;

DSGVO Art. 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Fortsetzung)

g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3)Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,

b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,

c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

(4)Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(5)Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit

a) die betroffene Person bereits über die Informationen verfügt,

b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,

c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder

d) die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

DSGVO - Informationspflicht

DSGVO Art. 33 (Aufsichtsbehörde) **& 34** (Betroffene)
"**Informationspflicht Datenschutzverletzung**"

- Information an Aufsichtsbehörde ("möglichst binnen 72 Stunden", mit Begründung später)
- unverzügliche persönliche Information an Betroffenen (bei "hohem Risiko für die persönlichen Rechte und Freiheiten")

Informationsinhalt an Aufsichtsbehörde und Betroffenen (soweit möglich)

- Beschreibung der Art der Verletzung [beide]
- Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze [Aufsicht]
- Name und Kontaktstelle (Datenschutzbeauftragter oder sonstige Anlaufstelle) [beide]
- Beschreibung der wahrscheinlichen Folgen für Betroffene [beide]
- Beschreibung der ergriffenen Maßnahmen [beide]

VO SS2019 - Juridicum

DSGVO Art. 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1)Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2)Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

(3)Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4)Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5)Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

DSGVO Art. 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1)Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

(2)Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

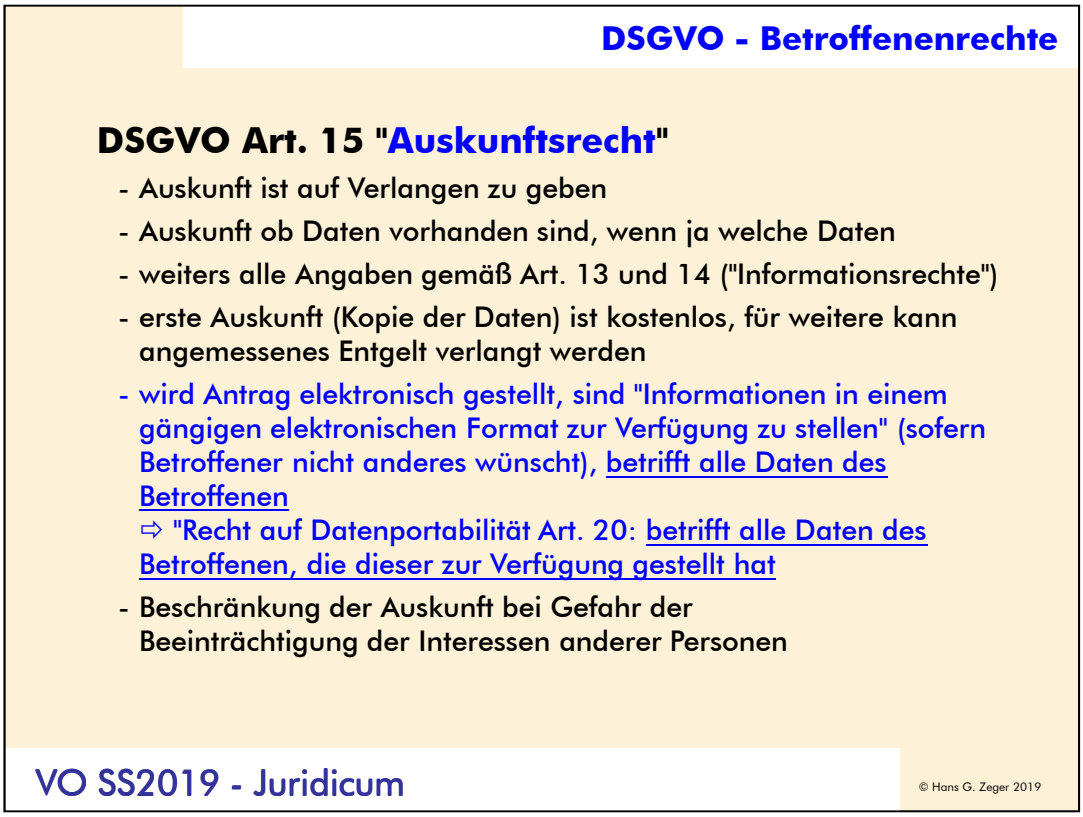
(3)Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;

b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4)Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.



DSGVO Art. 15 Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

DSGVO - Betroffenenrechte

DSGVO Art. 15 "Auskunftsrecht" II

Abweichung zum DSG 2000

- KEINE Beschränkung auf jährlich und/oder "aktuelle" Daten
- KEIN spezifischer Identitätsnachweis erforderlich, aber zusätzliche Identitätsangaben können bei "begründeten Zweifel" gefordert werden
- KEINE Formvorgaben bei Auskunftsbegehren
- KEIN "therapeutisches" Privileg: "Recht auf Auskunft über diese personenbezogenen Daten"
- Auskunft über Auftragsverarbeiter inkludiert
- KEINE spezifische Mitwirkungspflicht des Betroffenen, aber Auskunftsverweigerungsrecht bei "exzessiven Anträgen"
- KEINE gesetzliche Beschränkung zulässig

Fristen und allgemeine Verfahrensregeln in Art. 12 geregelt

VO SS2019 - Juridicum

DSGVO Art. 15 Auskunftsrecht der betroffenen Person (Fortsetzung)

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 1b darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Entscheidung - Auskunftsrecht

DSG: OGH 6Ob25/90 ("Schikaneverbot")

Ausgangslage

- Betroffener verlangte Auskunft bei einer Bank
- Auskunft wurde über "Stammdaten" gegeben, nicht jedoch Buchungsdaten
- Bank: "Buchungsdaten seien im Rahmen der Kontoauszüge schon einmal übermittelt"

OGH-Entscheidung

- folgt Argumentation der Bank

DSGVO: DSB nicht öffentlich ("Vorrang")

Ausgangslage

- Betroffener verlangte alte Kontoauszüge
- Bank wollte für Gebühren
- Betroffener verlangte kostenlos alte Kontoauskünfte auf Basis Art. 15 DSGVO
- Auskunft verweigert

DSB-Entscheidung

- DSGVO-Auskunftsanspruch hat als Rechtsanspruch Vorrang gegenüber anderen Regelungen

VO SS2019 - Juridicum

-

DSGVO Art. 16 Recht auf Berichtigung

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

DSGVO Art. 17 Recht auf Löschung („Recht auf Vergessenwerden")

(1)Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

DSGVO - Betroffenenrechte

DSGVO Art. 17 "Recht auf Löschung" II

Verpflichtung bei öffentlich zugänglichen Daten Verantwortliche zu informieren, dass die "Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten" verlangt wurde ["Lex Facebook/Schrems"]

Beschränkung der Löschung

- Informationen dienen der Ausübung der freien Meinungsäußerung
- Verwendung ist auf Grund von Rechtsvorschriften erforderlich
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke
- für statistische Zwecke
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen [des Verantwortlichen]

VO SS2019 - Juridicum

DSGVO Art. 17 Recht auf Löschung („Recht auf Vergessenwerden“)

(2)Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

(3)Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;

d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder

e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Entscheidung - Löschung

DSB-D123.270/0009-DSB/2018 ("Anonymisierung")

Ausgangslage

- Nutzer eines Online-Beratungsforums verlangte Löschung
- Forum löschte ein konkretes Offert + Kontaktdaten des Betroffenen
- sonstige Daten, insbesondere Identifikaitonsdaten wurden durch anonyme Personenkennung überschrieben
- Löschen der personenbezogenen Kundenhistorie

DSB-Entscheidung

- wenn bei Daten durch Anonymisierung sicher gestellt ist, dass kein Personenbezug wiederhergestellt werden kann, entspricht das der Löschung

⇨ Bedeutung in komplexen Datenbanksystemen zu Erhalt der technischen Systemintegrität

⇨ Erlaubt weitere Kundennutzung für komplexe Marketing- und Systemanalysen

VO SS2019 - Juridicum

DSB-D123.270/0009-DSB/2018

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von Dr. Xaver X**** (Beschwerdeführer) vom 27. Juli 2018 gegen die **** AG (Beschwerdegegnerin) wegen Verletzung im Recht auf Löschung wie folgt:

- Die Beschwerde wird abgewiesen.

Rechtsgrundlagen: Art. 2 Abs. 1, Art. 17 Abs. 1, Art. 55 Abs. 1, Art. 57 Abs. 1 lit. f sowie Art. 77 Abs. 1 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), ABl. Nr. L 119 S. 1; § 24 Abs. 1 und 5 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999 idgF

...

4. Nach Aufforderung der Datenschutzbehörde legte die Beschwerdegegnerin mit Stellungnahme vom 3. Oktober 2018 ihren Anonymisierungsprozess dar. So sei – zusammengefasst – die ursprüngliche Kundenverbindung („KUV") im Rahmen der Anfrage des Beschwerdeführers durch Umsetzung folgender kombinierter Schritte aus Löschung und Anonymisierung entfernt worden:

1) Löschung des Offerts: Sowohl die Kundenanfrage als auch das Angebot, das aufgrund der Onlineangaben des Kunden vom Kundenmanagementsystem erstellt worden wären, wären gelöscht worden.

2) Löschung aller elektronischer Kontakte (E-Mail-Adresse, Telefonnummer, etc.) des Kunden.

3) Änderung der Person (Name, Vorname, Adresse): Sowohl Name, als auch Adresse seien durch eine anonyme, nicht zuordenbare Person (Max Mustermann) mit identem Geschlecht und Geburtsdatum unwiderruflich manuell überschrieben worden.

4) Die nun inhaltsleere Kundenverbindung sei nur mehr Max Mustermann zugeordnet.

5) Der mit einer Kundenverbindung automatisch gestartete interne Ablauf sei sofort gestoppt worden.

6) Zusammenlegung der zu löschenden Person auf die neue anonyme Person zur Sicherstellung, dass die Überschreibung auch technisch nachhaltig verankert sei.

7) Löschen des Kunden im Elektronischen Akt (Historie).

Durch die Umsetzung all dieser beschriebenen Schritte sei eine faktische Anonymisierung der ursprünglichen Kundenverbindung durch das Überschreiben mit einer „Dummy Kundenverbindung" herbeigeführt worden. Es wären nunmehr keine personenbezogenen Daten und somit keine identifizierenden Merkmale vorhanden, die mit der ursprünglichen Onlineanfrage des Kunden in Verbindung gebracht werden könnten. Vielmehr bestünde nur mehr eine inhaltsleere Kundenverbindung zu Max Mustermann und wären somit keine weiteren Informationen vorhanden, die auf den Beschwerdeführer hinweisen würden. Auch rechtlich entspreche die so durchgeführte, dargestellte Anonymisierung personenbezogener Daten einer dauerhaften Löschung, da die Daten damit nicht mehr personenbezogen und sohin dem Anwendungsbereich der DSGVO entzogen wären.

DSGVO - Betroffenenrechte

DSGVO Art. 18 "Recht auf Einschränkung"

- Richtigkeit der Daten wird bestritten, für die Dauer der Klärung des Sachverhalts
- die Verarbeitung ist rechtswidrig, der Betroffene lehnt jedoch die Löschung ab und verlangt eine Beschränkung der Verwendung
- Verantwortliche benötigt die Daten nicht länger, aber Betroffener benötigt sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

Im Fall einer Einschränkung dürfen Daten "*nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden*"

VO SS2019 - Juridicum

DSGVO Art. 18 Recht auf Einschränkung der Verarbeitung

(1)Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

a) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,

b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

c) der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

d) die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

(2)Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten — von ihrer Speicherung abgesehen — nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

(3)Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird.

DSGVO - Informationspflicht

DSGVO Art. 19 "Informationspflicht Datenänderung"

- Empfänger von Daten werden informiert, bei
  jeder Berichtigung (Art. 16) oder Löschung (Art. 17 Abs. 1)
  personenbezogener Daten oder
  einer Einschränkung der Verarbeitung (Art. 18)

Ausnahme von Informationspflicht

- Verständigung ist unmöglich
- Aufwand ist unverhältnismäßig

Informationsrecht des Betroffenen

- auf Verlangen sind Betroffene über Empfänger zu informieren

VO SS2019 - Juridicum

DSGVO Art. 19 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Der Verantwortliche teilt allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 18 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

DSGVO Art. 20 "Datenportabilität"

- Recht auf Erhalt eigener Daten in "strukturiertem, gängigen und maschinenlesbarem Format zu erhalten"
- Recht auf Übermittlung dieser Daten an einen anderen Verantwortlichen

Voraussetzungen

- Verarbeitung erfolgt auf Grund einer Einwilligung (Art. 6 Abs. 1 lit a oder Art. 9 Abs. 2 lit a) oder
- Verarbeitung erfolgt auf Grund eines Vertrages (Art. 6 Abs. 1 lit b)
- \+ Verarbeitung erfolgt automatisiert
- \+ Grundrechte Dritter werden nicht beeinträchtigt

geeignete Maßnahmen

- Anspruch der direkten Übertragung von einem Verantwortlichen an einen anderen
- Löschungsrecht (Art. 17) bleibt davon unberührt

Anwendungsbereiche: Kontoübertragungen, KFZ-Daten, SocialMedia-Accounts, Mobiltelefonie, Clouddienste!

DSGVO Art. 20 Recht auf Datenübertragbarkeit

(1)Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und

b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

(2)Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

(3)Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(4)Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

DSGVO Art. 22 "Profiling & Einzelentscheidung"

- Recht keiner rechtlichen, ausschließlich automatisierten Einzelentscheidung oder Profiling unterworfen zu werden

Ausnahmen (wenn geeignete Maßnahmen ergriffen werden)

- für den Abschluss eines Vertrages erforderlich
- auf Grund von Rechtsvorschriften zulässig
- mit ausdrücklicher Einwilligung des Betroffenen

geeignete Maßnahmen

- Anfechtung der Entscheidung ist möglich
- Betroffener kann Standpunkt darlegen
- Einschränkung in der Verwendung besonderer Kategorien von Daten

DSGVO Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1)Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2)Absatz 1 gilt nicht, wenn die Entscheidung

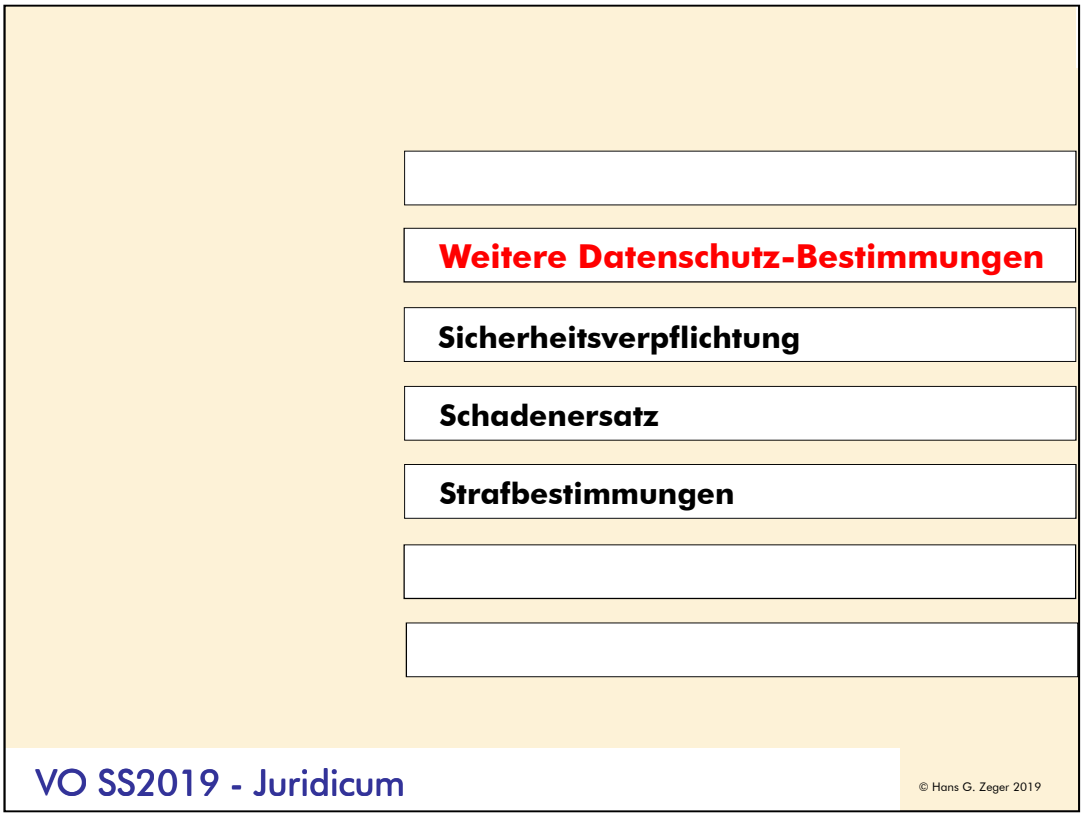
a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,

b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

(3)In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4)Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.


Weitere Datenschutz-Bestimmungen
Sicherheitsverpflichtung
Schadenersatz
Strafbestimmungen
VO SS2019 - Juridicum
© Hans G. Zeger 2019

-

DSGVO - Sicherheit

DSGVO Art. 32 "Sicherheit"

Grundsatz der Verhältnismäßigkeit (Abs 1):

- Stand der Technik
- Implementierungskosten
- Zwecke der Verarbeitung
- unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

individuelle Vertragsklauseln zwischen Verantwortlichen oder dem Auftragsverarbeiter und Empfänger (Art. 46 Abs. 3 lit a)

zu setzende Maßnahmen

- Pseudonymisierung und Verschlüsselung personenbezogener Daten (Abs 1 lit a)
- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste müssen auf Dauer sichergestellt sein (Abs 1 lit b)
- Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen muss nach einem Zwischenfall rasch wieder hergestellt werden (Abs 1 lit c)

VO SS2019 - Juridicum

DSGVO Art. 32 Sicherheit der Verarbeitung

(1)Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2)Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3)Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

DSGVO Art. 32 "Sicherheit" II

zu setzende Maßnahmen (Fortsetzung)

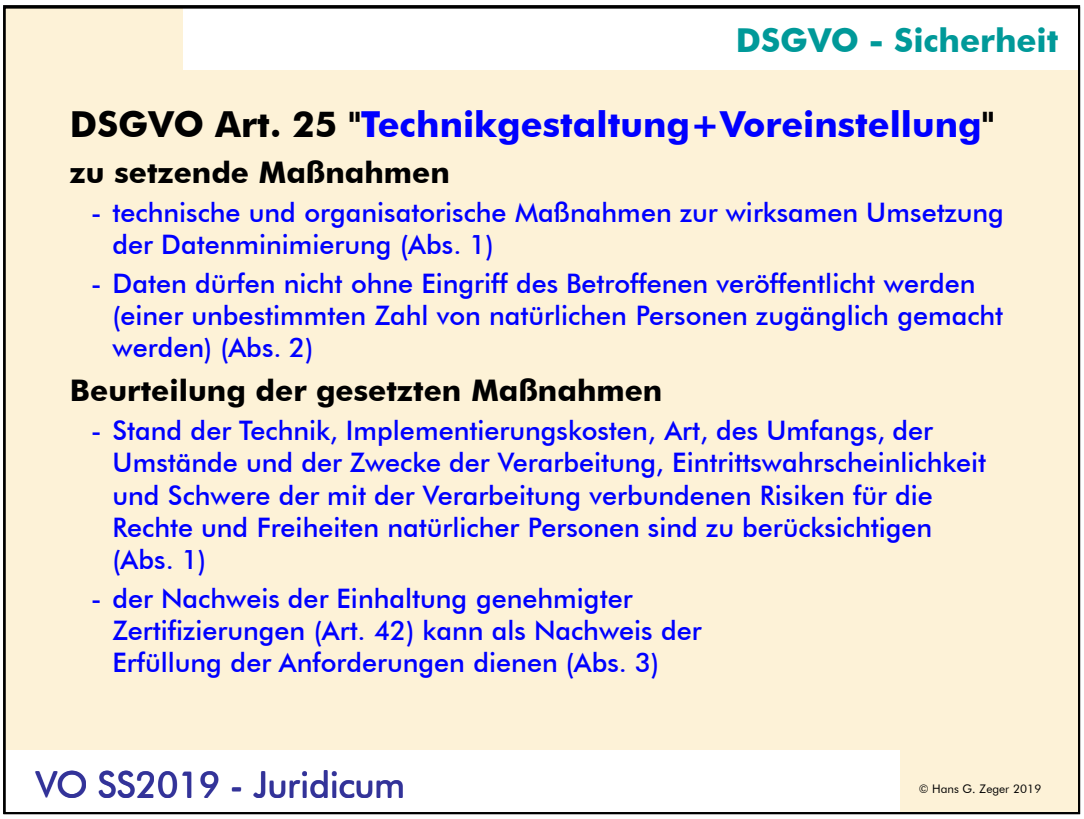
- Implementierung von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Abs. 1 lit d)
- Sicherung, dass Mitarbeiter Daten nur gemäß Anweisungen verwenden (Abs. 4)

Beurteilung der gesetzten Maßnahmen

- bei Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind (Abs. 2)
- der Nachweis der Einhaltung genehmigter Verhaltensregeln (Art. 40) oder genehmigter Zertifizierungen (Art. 42) kann als Nachweis der Erfüllung der Anforderungen dienen (Abs. 3)

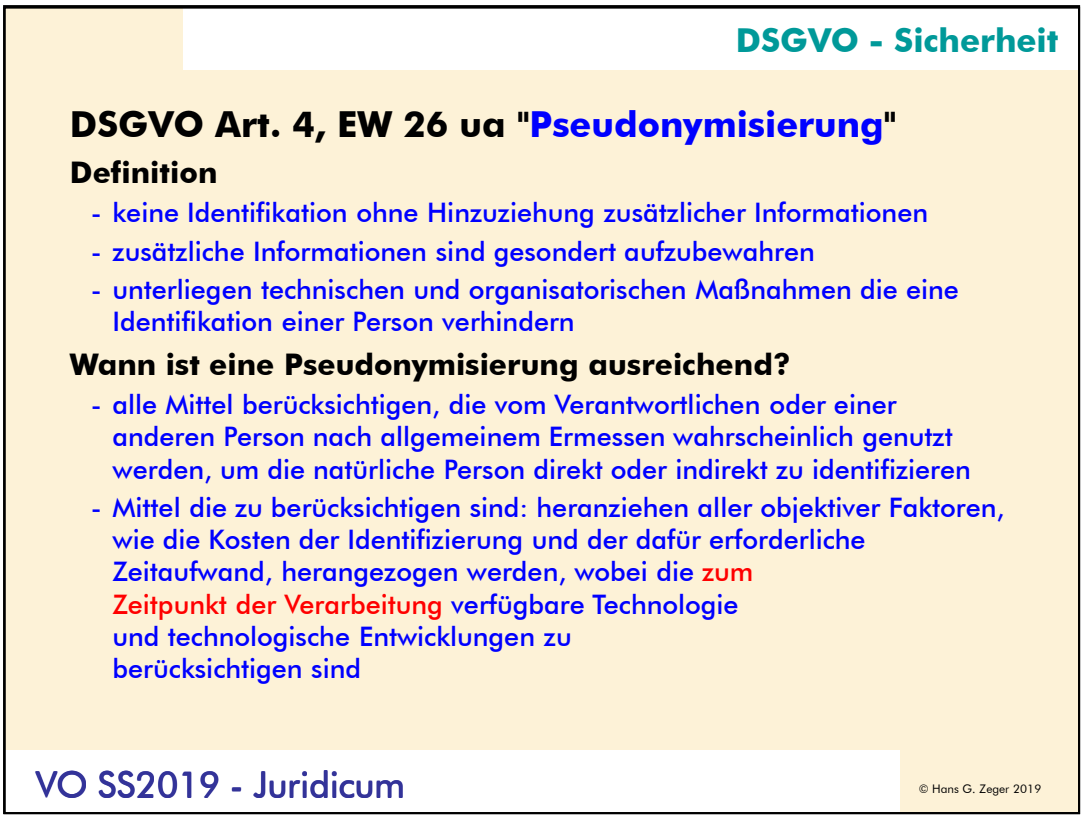
DSGVO Art. 32 Sicherheit der Verarbeitung (Fortsetzung)

(4)Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.



DSGVO *Artikel 25* Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1)Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. (2)Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. (3)Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

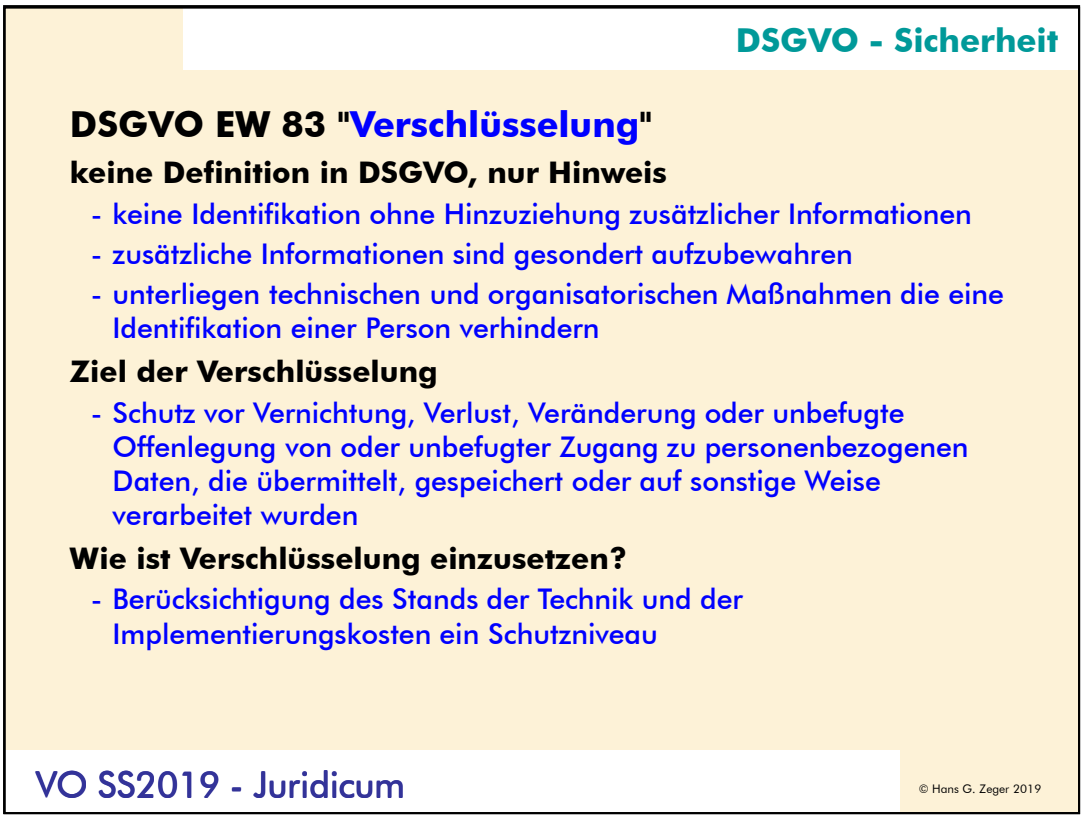


DSGVO Art. 4 Begriffsbestimmungen

5. „**Pseudonymisierung**“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten **ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen**, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

EW 26

Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. ***Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.*** Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.



EW 83

Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau — auch hinsichtlich der Vertraulichkeit — gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte.

DSGVO - Sicherheit

Konsequenzen der Sicherheitsvorgaben gemäß DSGVO

- keine Verpflichtung eine bestimmte Technik einzusetzen
- umfassende Verpflichtung bei jeden Verarbeitungsschritt konkrete Sicherheitsmaßnahmen umzusetzen, insbesondere Pseudonymisierung, Verschlüsselung
- laufende Prüfung ob Maßnahmen noch geeignet sind

Die Maßnahmen werden bei Verarbeitungen mit "besonderen Datenkateorien" oder ab einer gewissen Verarbeitungskomplexität nicht ohne eine umfassende Security-Policy umsetzbar sein!

geeignete Grundlagen einer Security Policy

- BSI M 2.192 Erstellung einer IT-Sicherheitsleitlinie
- ISO 27001 Informationssicherheitsleitlinie
- österreichisches Informations-Sicherheitshandbuch
- genehmigte Verhaltensregeln gemäß Art. 40 DSGVO
- Empfehlungen des "European Data Protection Board"

VO SS2019 - Juridicum

Beachtung technischer Maßnahmen

laufende Beobachtung diverser Mailinglisten (CERT),

Publikationen der Art. 29 Datenschutzgruppe der EU,

Anlehnung an bestehende Konzepte und Empfehlungen
BSI-Handbuch, IT-Sicherheitshandbücher, Datenschutzgütesiegel

Befassung externer Berater (Wirtschaftstreuhänder, Sicherheitsberater, ...),

Outsourcing einzelner IT-Sicherheitsaspekte an ISP, Dienstleister
SPAM- und Viren/Wurm-Kontrolle, Firewall, ...

Arbeitspapiere der Art. 29 Gruppe

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

Auswahl:

- verbindlichen unternehmensinternen Datenschutzregelungen für Auftragsverarbeiter (Binding Corporate Rules)
- Arbeitspapier über genetische Daten
- unerbetenen Werbenachrichten
- Verarbeitung personenbezogener Daten aus der Videoüberwachung
- vertrauenswürdige Rechnerplattformen

Sicherheitsbestimmungen

DSGVO Art. 5 "Rechenschaftspflicht"

- keine komplizierte Protokollierungsverpflichtung wie im DSG 2000!
- JEDOCH! Nachweispflicht der Einhaltung aller Verarbeitungsgrundsätze gemäß Art. 5
- DSG lässt jedoch Protokollierungspflicht bei Bildverarbeitung wiederauferstehen!

Konsequenzen der Rechenschaftspflicht

- gesamte Verarbeitung personenbezogener Daten muss auditierbar sein
- Unterlagen müssen revisionssicher gestaltet werden
- zeitliche Zuordnung der Abläufe muss qualifiziert und fälschungssicher erfolgen (zB Zeitstempeldienste)

VO SS2019 - Juridicum

-

DSG - Bestimmungen

DSG § 6 "Datengeheimnis"

Mitarbeiter sind zum Datengeheimnis zu verpflichten

Mitarbeiter sind über Folgen der Verletzung des Datengeheimnisses zu belehren

Daten dürfen nur auf Grund ausdrücklicher Anordnung verwendet werden

Mitarbeiter darf aus der Weigerung einer rechtswidrigen Übermittlung kein Nachteil erwachsen

bestehende gesetzliche Aussageverweigerungsrechte dürfen nicht durch Inanspruchnahme eines für den Verantwortlichen tätigen Auftragsverarbeiters umgangen werden

VO SS2019 - Juridicum

Datengeheimnis

DSG § 6. (1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

DSGVO - Kontroll- & Strafbestimmungen

DSGVO Art. 82 "Schadenersatz"

- schuldhaftes Verhalten erforderlich
- es ist materieller UND immaterieller Schaden zu ersetzen
- sind mehrere Verantwortliche beteiligt, haftet jeder ungeteilt

Unterschied der DSGVO zum DSG 2000 Schadenersatz

KEINE bestimmten Schadenshöhen vorgegeben

KEINE Einschränkungen in der Art des Schadens (DSG 2000: nur bei bloßstellender Datenschutzverletzung)

KEIN Bezug auf andere Bestimmungen (wie Medienrecht)

Schuldhaftes Handeln = Vorsatz oder fahrlässiges Handeln

VO SS2019 - Juridicum

DSGVO Art. 82 Haftung und Recht auf Schadenersatz

(1)Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

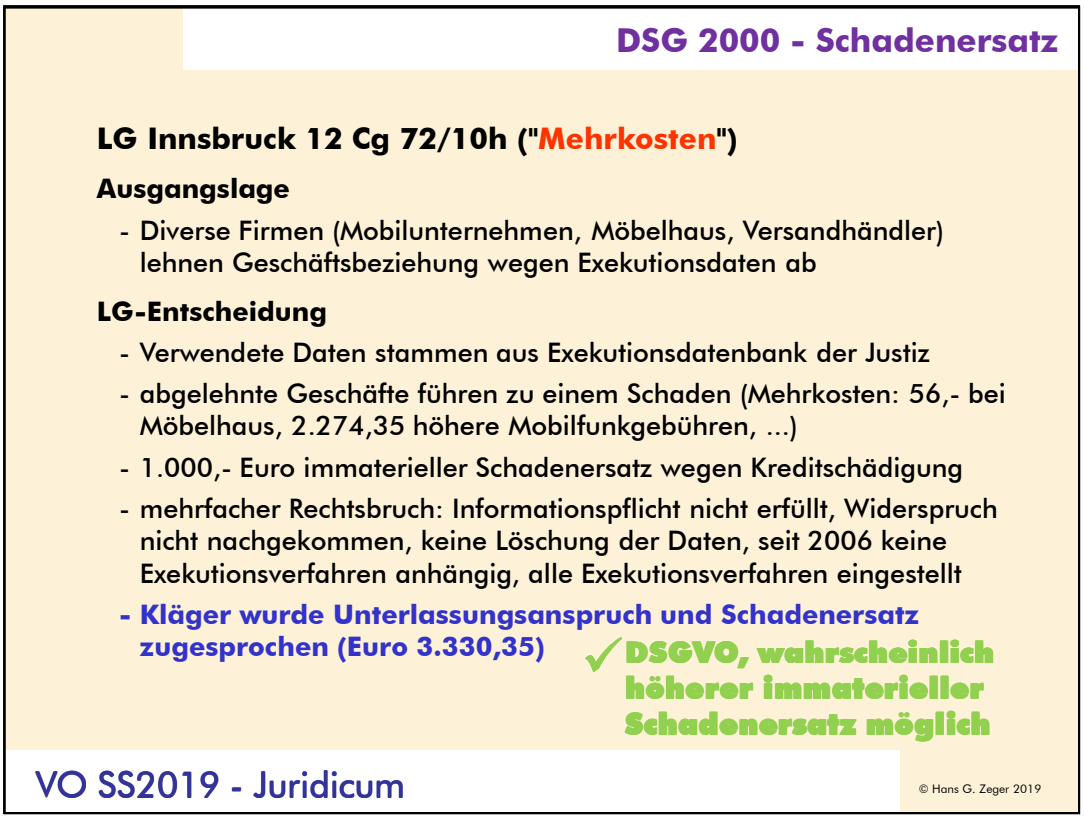
(2)Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

(3)Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4)Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

(5)Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6)Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.



LG Innsbruck 12 Cg 72/10h

Die beklagte Partei ist schuldig, dem Kläger binnen 14 Tagen zu Handen der Klagsvertreterin einen Betrag von EUR 3.330,35 samt 4 % Zinsen aus EUR 3.331,40 vom 11.2.2010 bis 2.6.2010 sowie 4 % Zinsen aus EUR 3.330,35 ab dem 3.6.2010 zu bezahlen und die mit EUR 1.448,80 (darin enthalten EUR 316,-- Barauslagen und EUR 188,80 USt) bestimmten Verfahrenskosten zu ersetzen. ...

Durch die rechtswidrige und schuldhafte Verwendung der Bonitätsdaten des Klägers sei diesem ein Schaden durch erhöhte Mobilfunkgebühren bis Mai 2009 in Höhe von EUR 2.274,35 entstanden, weiters ein Schaden durch Mehrkosten, weil er einen Kinderwagen nicht online bei der Firma Eduscho sondern in der Folge bei der Firma Kika im August 2008 kaufen habe müssen in Höhe von EUR 56,-- und weiters habe der Kläger Strafporto in Höhe von EUR 1,05 bezahlen müssen, da der Beklagte einen an den Kläger adressierten Brief wegen Auskunft nach dem Datenschutzgesetz nicht frankiert habe, obwohl er hiezu nach dem Datenschutzgesetz verpflichtet gewesen wäre.

Weiters begehrte der Kläger eine angemessene Entschädigung in Höhe von EUR 1.000,-- für die erlittene Kränkung, weil durch die öffentliche zugängliche rechtswidrige Verwendung der über den Kläger gespeicherten Datensätze und Übermittlung derselben an verschiedene Personen schutzwürdige Geheimhaltungsinteressen des Klägers vom Beklagten verletzt worden seien und der Kläger gegenüber mehreren Firmen bloßgestellt worden sei.

DSGVO - Strafbestimmungen

DSGVO Art. 58, 83, 84 "Sanktionen"

- Aufsichtsbehörden sind verantwortlich für wirksame, verhältnismäßige und abschreckende Sanktionen (Art. 83 Abs 1)
- umfassende Untersuchungs-, Abmahn- und Abhilfebefugnisse inkl. der Möglichkeit eine Datenverarbeitung zu verbieten (Art. 58)
- Geldbußen haben ua Art, Schwere und Dauer eines Verstoßes zu berücksichtigen, Vorsätzlichkeit oder Fahrlässigkeit, Grad der Verantwortung, frühere Verstöße, Kategorien der betroffenen Daten

Geldbußen bis 10 Mio EUR (Art. 83 Abs. 4)
(bei Unternehmen bis 2% seines gesamten weltweit erzielten Jahresumsatzes)

- Missachtung der Datenschutz-Rechte eines Kindes (iS Art. 8)
- Verarbeitung von personenbezogenen Daten, obwohl Identifizierung nicht erforderlich (iS Art. 11)
- sonstige allgemeine Verletzungen bei Datenverarbeitungen inkl. Verletzung von Sicherheitsbestimmungen (iS Art. 25-39)

VO SS2019 - Juridicum

DSGVO Art. 83 Allgemeine Bedingungen für die Verhängung von Geldbußen

(1)Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2)Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;

f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

i)Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und

k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

DSGVO - Strafbestimmungen

DSGVO Art. 58, 83, 84 "Sanktionen" II

Geldbußen bis 20 Mio EUR (Art. 83 Abs. 5)
(bei Unternehmen bis 4% seines gesamten weltweit erzielten Jahresumsatzes)

- Verletzung von Verarbeitungsgrundsätzen (iS Art. 5, 6, 7, 9)
- Verletzung der Betroffenenrechte (iS Art. 12-22)
- unzulässige Datenübermittlung in Drittländer oder internationale Organisationen (iS Art. 44-49)
- Missachtung der Regeln für besondere Verarbeitungssituationen (etwa zu Meinungsfreiheit) (iS Kapitel IX Art. 85-91)
- Verhinderung oder Behinderung von Untersuchungen der Aufsichtsbehörden (iS Art. 58 Abs. 1,2)
- Nichtbefolgung von Anweisungen der Aufsichtsbehörden (iS Art. 58 Abs. 2)

VO SS2019 - Juridicum

DSGVO Art. 83 Allgemeine Bedingungen für die Verhängung von Geldbußen (Fortsetzung)

(3)Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4)Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5)Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;

c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6)Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

Allgemeine Bedingungen für die Verhängung von Geldbußen

§ 30. (1) Die Datenschutzbehörde kann Geldbußen gegen eine juristische Person verhängen, wenn Verstöße gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück durch Personen begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt haben

und eine Führungsposition innerhalb der juristischen Person aufgrund

1. der Befugnis zur Vertretung der juristischen Person,

2. der Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder

3. einer Kontrollbefugnis innerhalb der juristischen Person innehaben.

(2) Juristische Personen können wegen Verstößen gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück auch verantwortlich gemacht werden, wenn mangelnde Überwachung oder Kontrolle durch eine in Abs. 1 genannte Person die Begehung dieser Verstöße durch eine für die juristische Person tätige Person ermöglicht hat, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet.

(3) Die Datenschutzbehörde hat von der Bestrafung eines Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991 – VStG, BGBl. Nr. 52/1991, abzusehen, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird.

(4) Die gemäß § 22 Abs. 5 verhängten Geldbußen fließen dem Bund zu und sind nach den Bestimmungen über die Eintreibung von gerichtlichen Geldstrafen einzubringen. Rechtskräftige Bescheide der Datenschutzbehörde sind Exekutionstitel. Die Bewilligung und der Vollzug der Exekution ist auf Grund des Exekutionstitels der Datenschutzbehörde bei dem Bezirksgericht, in dessen Sprengel der Verpflichtete seinen allgemeinen Gerichtsstand in Streitsachen hat (§§ 66, 75 der Jurisdiktionsnorm – JN, RGBl. Nr. 111/1895), oder bei dem in den §§ 18 und 19 EO bezeichneten Exekutionsgericht zu beantragen.

(5) Gegen Behörden und öffentliche Stellen, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, die im gesetzlichen Auftrag handeln, und gegen Körperschaften des öffentlichen Rechts können keine Geldbußen verhängt werden.

DSGVO / DSG - Strafbestimmungen

DSG § 62 "ergänzende Sanktionen" II

- Verweigerung der Einschau durch die Datenschutzbehörde
- Versuch ist strafbar
- Verfall von Datenträgern und Programmen kann ausgesprochen werden, wenn diese im Zusammenhang mit der Verwaltungsübertretung stehen
- verschaffen von personenbezogenen Daten unter Vortäuschung falscher Tatsachen
- Datenschutzbehörde ist zuständige Strafbehörde

DSB Strafpraxis 2018

- **59 Straf-Entscheidungen nach DSGVO / DSG**
- **inhaltlich bekannt wurden zwei Entscheidungen, beide zur Videoüberwachung**
- **bisher höchste Strafe 6.700,- Euro**

VO SS2019 - Juridicum

Verwaltungsstrafbestimmung

§ 62. (1) Sofern die Tat nicht einen Tatbestand nach Art. 83 DSGVO verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 50 000 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenverarbeitung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält,

2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 6) übermittelt, insbesondere Daten, die ihm gemäß §§ 7 oder 8 anvertraut wurden, vorsätzlich für andere unzulässige Zwecke verarbeitet,

3. sich unter Vortäuschung falscher Tatsachen vorsätzlich personenbezogene Daten gemäß § 10 verschafft,

4. eine Bildverarbeitung entgegen den Bestimmungen des 3. Abschnittes des 1. Hauptstücks betreibt oder

5. die Einschau gemäß § 22 Abs. 2 verweigert.

(2) Der Versuch ist strafbar.

(3) Gegen juristische Personen können bei Verwaltungsübertretung nach Abs. 1 und 2 Geldbußen nach Maßgabe des § 30 verhängt werden.

(4) Die Strafe des Verfalls von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 in Zusammenhang stehen.

(5) Die Datenschutzbehörde ist zuständig für Entscheidungen nach Abs. 1 bis 4.

DSG - Strafbestimmungen

DSG § 63 "Strafrecht"

- Datenverarbeitung in Gewinn- oder Schädigungsabsicht

Delikt begeht, wer vorsätzlich ...

- widerrechtlich ihm zugängliche Daten benutzt **oder**
- Daten widerrechtlich beschafft **oder**
- anderen widerrechtlich zugänglich macht **oder**
- widerrechtlich öffentlich macht

Strafausmaß: bis ein Jahr oder Geldstrafe bis 720 Tagessätze
Delikt ist Offizialdelikt
Strafbestimmung gilt subsidiär

VO SS2019 - Juridicum

Datenverarbeitung in Gewinn- oder Schädigungsabsicht

DSG § 63. Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

Missbrauch der Amtsgewalt

StGB § 302. (1) Ein Beamter, der mit dem Vorsatz, dadurch einen anderen an seinen Rechten zu schädigen, seine Befugnis, im Namen des Bundes, eines Landes, eines Gemeindeverbandes, einer Gemeinde oder einer anderen Person des öffentlichen Rechtes als deren Organ in Vollziehung der Gesetze Amtsgeschäfte vorzunehmen, wissentlich mißbraucht, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) Wer die Tat bei der Führung eines Amtsgeschäfts mit einer fremden Macht oder einer über- oder zwischenstaatlichen Einrichtung begeht, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen. Ebenso ist zu bestrafen, wer durch die Tat einen 50 000 Euro übersteigenden Schaden herbeiführt.

Verletzung des Amtsgeheimnisses

StGB § 310. (1) Ein Beamter oder ehemaliger Beamter, der ein ihm ausschließlich kraft seines Amtes anvertrautes oder zugänglich gewordenes Geheimnis offenbart oder verwertet, dessen Offenbarung oder Verwertung geeignet ist, ein öffentliches oder ein berechtigtes privates Interesse zu verletzen, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer als Mitglied eines Ausschusses gemäß Art. 53 B-VG bzw. eines nach Art. 52a B-VG eingesetzten ständigen Unterausschusses oder als zur Anwesenheit bei deren Verhandlungen Berechtigter ein ihm in vertraulicher Sitzung zugänglich gewordenes Geheimnis offenbart oder verwertet, dessen Offenbarung oder Verwertung geeignet ist, ein öffentliches oder ein berechtigtes privates Interesse zu verletzen.

(2a) Ebenso ist zu bestrafen, wer - sei es auch nach seinem Ausscheiden aus dem Amt oder Dienstverhältnis - als Organwalter oder Bediensteter des Europäischen Polizeiamtes (Europol), als Verbindungsbeamter oder als zur Geheimhaltung besonders Verpflichteter (Art. 32 Abs. 2 des Europol-Übereinkommens, BGBl. III Nr. 123/1998) eine Tatsache oder Angelegenheit offenbart oder verwertet, die ihm ausschließlich kraft seines Amtes oder seiner Tätigkeit zugänglich geworden ist und deren Offenbarung oder Verwertung geeignet ist, ein öffentliches oder ein berechtigtes privates Interesse zu verletzen.

(3) Offenbart der Täter ein Amtsgeheimnis, das verfassungsgefährdende Tatsachen (§ 252 Abs. 3) betrifft, so ist er nur zu bestrafen, wenn er in der Absicht handelt, private Interessen zu verletzen oder der Republik Österreich einen Nachteil zuzufügen. Die irrtümliche Annahme verfassungsgefährdender Tatsachen befreit den Täter nicht von Strafe.

DSG - Meinungsfreiheit

DSGVO EW 153, Art. 85 "Meinungsfreiheit"

- Gestaltungsauftrag an Mitgliedstaaten "Meinungsfreiheit" und "Privatsphäre" in Einklang zu bringen

Gestaltungsspielraum ("Abweichungen und Ausnahmen" in einzelnen Kapitel):

- Kapitel II (Grundsätze, 5-11): ua "Zweckbindung", "Verarbeitungserlaubnis", "Einwilligung", ...
- Kapitel III (Rechte der betroffenen Person, 12-23): ua "Auskunftsrecht", "Löschungsrecht", ...
- Kapitel IV (Verantwortlicher und Auftragsverarbeiter, 24-43): ua "Verarbeitungsverzeichnis", "Folgenabschätzung", "Sicherheitsbestimmungen", ...
- Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen, 44-50)
- Kapitel VI (Unabhängige Aufsichtsbehörden, 51-59)
- Kapitel VII (Zusammenarbeit und Kohärenz, 60-76)
- Kapitel IX (Vorschriften für besondere Verarbeitungssituationen, 85-91)

VO SS2019 - Juridicum

DSGVO Art 85 Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit

(1)Die Mitgliedstaaten bringen durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang.

(2)Für die Verarbeitung, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, sehen die Mitgliedstaaten Abweichungen oder Ausnahmen von Kapitel II (Grundsätze), Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) vor, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.

(3)Jeder Mitgliedstaat teilt der Kommission die Rechtsvorschriften, die er aufgrund von Absatz 2 erlassen hat, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften mit.

DSG - Meinungsfreiheit

DSGVO EW 153, Art. 85 "Meinungsfreiheit" II

Was macht Österreich aus diesem Auftrag?

DSG § 9 Abs 1:

- Kapitel II, III, IV, V, VI, VII und IX sind pauschal **NICHT** anzuwenden!
- gilt für die Verarbeitung von personenbezogenen Daten durch **ALLE** Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens oder Mediendienstes im Sinne des Mediengesetzes – MedienG, BGBl. Nr. 314/1981, zu journalistischen Zwecken des Medienunternehmens oder Mediendienstes

VO SS2019 - Juridicum

Freiheit der Meinungsäußerung und Informationsfreiheit

DSG § 9. (1) Auf die Verarbeitung von personenbezogenen Daten durch Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens oder Mediendienstes im Sinne des Mediengesetzes – MedienG, BGBl. Nr. 314/1981, zu journalistischen Zwecken des Medienunternehmens oder Mediendienstes finden die Bestimmungen dieses Bundesgesetzes sowie von der DSGVO die Kapitel II (Grundsätze), III (Rechte der betroffenen Person), IV (Verantwortlicher und Auftragsverarbeiter), V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), VI (Unabhängige Aufsichtsbehörden), VII (Zusammenarbeit und Kohärenz) und IX (Vorschriften für besondere Verarbeitungssituationen) keine Anwendung. Die Datenschutzbehörde hat bei Ausübung ihrer Befugnisse gegenüber den im ersten Satz genannten Personen den Schutz des Redaktionsgeheimnisses (§ 31 MedienG) zu beachten.

(2) Soweit dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen, finden von der DSGVO die Kapitel II (Grundsätze), mit Ausnahme des Art. 5, Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), mit Ausnahme der Art. 28, 29 und 32, Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) auf die Verarbeitung, die zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, keine Anwendung. Von den Bestimmungen dieses Bundesgesetzes ist in solchen Fällen § 6 (Datengeheimnis) anzuwenden.

DSG - Meinungsfreiheit

DSGVO EW 153, Art. 85 "Meinungsfreiheit" III

Wer fällt unter diese Ausnahme?

Mediengesetz § 1 Abs 1:

- Z8 "Medieninhaber": ... c) im Fall eines elektronischen Mediums dessen inhaltliche Gestaltung besorgt und dessen Ausstrahlung, Abrufbarkeit oder Verbreitung entweder besorgt oder veranlasst
- Z1 "Medium": jedes Mittel zur Verbreitung von Mitteilungen oder Darbietungen mit gedanklichem Inhalt in Wort, Schrift, Ton oder Bild an einen größeren Personenkreis im Wege der Massenherstellung oder der Massenverbreitung
- Z5a. "periodisches elektronisches Medium: Medium, das auf elektronischem Wege ... b) abrufbar ist (Website) ...

Formal bleibt die DSB als Aufsicht zuständig

DSG § 9 Abs 1:

- "Die Datenschutzbehörde hat bei Ausübung ihrer Befugnisse gegenüber den im ersten Satz genannten Personen den Schutz des Redaktionsgeheimnisses (§ 31 MedienG) zu beachten."

VO SS2019 - Juridicum

Begriffsbestimmungen

Mediengesetz § 1. (1) Im Sinn der Bestimmungen dieses Bundesgesetzes ist

1. „Medium“: jedes Mittel zur Verbreitung von Mitteilungen oder Darbietungen mit gedanklichem Inhalt in Wort, Schrift, Ton oder Bild an einen größeren Personenkreis im Wege der Massenherstellung oder der Massenverbreitung;

1a. „Medieninhalte“: Mitteilungen oder Darbietungen mit gedanklichem Inhalt in Wort, Schrift, Ton oder Bild, die in einem Medium enthalten sind;

2. „periodisches Medium“: ein periodisches Medienwerk oder ein periodisches elektronisches Medium;

3. „Medienwerk“: ein zur Verbreitung an einen größeren Personenkreis bestimmter, in einem Massenherstellungsverfahren in Medienstücken vervielfältigter Träger von Mitteilungen oder Darbietungen mit gedanklichem Inhalt;

4. „Druckwerk“: ein Medienwerk, durch das Mitteilungen oder Darbietungen ausschließlich in Schrift oder in Standbildern verbreitet werden;

5. „periodisches Medienwerk oder Druckwerk“: ein Medienwerk oder Druckwerk, das unter demselben Namen in fortlaufenden Nummern wenigstens viermal im Kalenderjahr in gleichen oder ungleichen Abständen erscheint und dessen einzelne Nummern, mag auch jede ein in sich abgeschlossenes Ganzes bilden, durch ihren Inhalt im Zusammenhang stehen;

5a. „periodisches elektronisches Medium“: ein Medium, das auf elektronischem Wege

a) ausgestrahlt wird (Rundfunkprogramm) oder

b) abrufbar ist (Website) oder

c) wenigstens vier Mal im Kalenderjahr in vergleichbarer Gestaltung verbreitet wird (wiederkehrendes elektronisches Medium);

6. „Medienunternehmen“: ein Unternehmen, in dem die inhaltliche Gestaltung des Mediums besorgt wird sowie

a) seine Herstellung und Verbreitung oder

b) seine Ausstrahlung oder Abrufbarkeit

entweder besorgt oder veranlasst werden;

7. „Mediendienst“: ein Unternehmen, das Medienunternehmen wiederkehrend mit Beiträgen in Wort, Schrift, Ton oder Bild versorgt;

8. „Medieninhaber“: wer

a) ein Medienunternehmen oder einen Mediendienst betreibt oder

b) sonst die inhaltliche Gestaltung eines Medienwerks besorgt und dessen Herstellung und Verbreitung entweder besorgt oder veranlasst oder

c) sonst im Fall eines elektronischen Mediums dessen inhaltliche Gestaltung besorgt und dessen Ausstrahlung, Abrufbarkeit oder Verbreitung entweder besorgt oder veranlasst oder

d) sonst die inhaltliche Gestaltung eines Mediums zum Zweck der nachfolgenden Ausstrahlung, Abrufbarkeit oder Verbreitung besorgt;

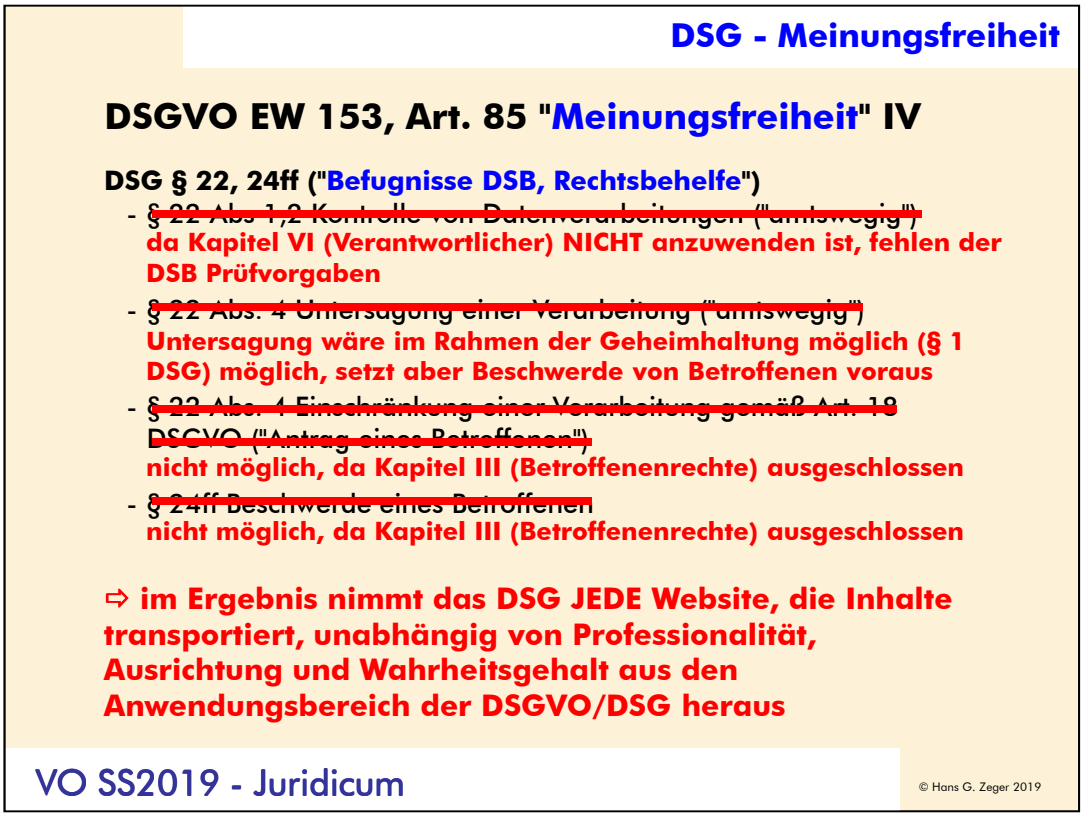
9. „Herausgeber“: wer die grundlegende Richtung des periodischen Mediums bestimmt;

10. „Hersteller“: wer die Massenherstellung von Medienwerken besorgt;

11. „Medienmitarbeiter“: wer in einem Medienunternehmen oder Mediendienst an der inhaltlichen Gestaltung eines Mediums oder der Mitteilungen des Mediendienstes journalistisch mitwirkt, sofern er als Angestellter des Medienunternehmens oder Mediendienstes oder als freier Mitarbeiter diese journalistische Tätigkeit ständig und nicht bloß als wirtschaftlich unbedeutende Nebenbeschäftigung ausübt;

12. „Medieninhaltsdelikt“: eine durch den Inhalt eines Mediums begangene, mit gerichtlicher Strafe bedrohte Handlung, die in einer an einen größeren Personenkreis gerichteten Mitteilung oder Darbietung besteht.

(2) Zu den Medienwerken gehören auch die in Medienstücken vervielfältigten Mitteilungen der Mediendienste. Im übrigen gelten die Mitteilungen der Mediendienste ohne Rücksicht auf die technische Form, in der sie geliefert werden, als Medien.



Befugnisse Datenschutzbehörde

DSG § 22. (1) Die Datenschutzbehörde kann vom Verantwortlichen oder Auftragsverarbeiter der überprüften Datenverarbeitung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenverarbeitungen und diesbezügliche Unterlagen begehren. Der Verantwortliche oder Auftragsverarbeiter hat die notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Verantwortlichen oder des Auftragsverarbeiters und Dritter auszuüben.

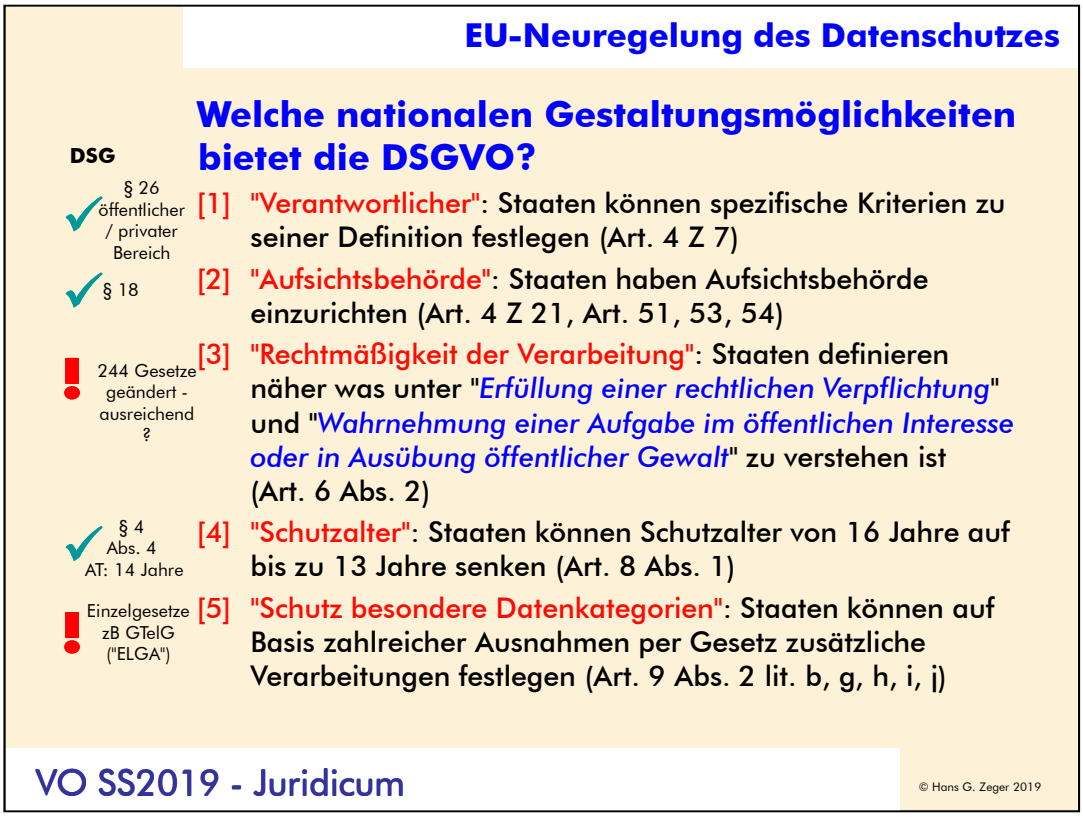
(2) Zum Zweck der Einschau ist die Datenschutzbehörde nach Verständigung des Inhabers der Räumlichkeiten und des Verantwortlichen oder des Auftragsverarbeiters berechtigt, Räume, in welchen Datenverarbeitungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen.

(3) Informationen, die der Datenschutzbehörde oder den von ihr Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Im Übrigen besteht die Pflicht zur Verschwiegenheit auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach § 63 dieses Bundesgesetzes oder nach §§ 118a, 119, 119a, 126a bis 126c, 148a oder § 278a des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974, oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch Ersuchen nach § 76 der Strafprozeßordnung – StPO, BGBl. Nr. 631/1975, zu entsprechen ist.

(4) Liegt durch den Betrieb einer Datenverarbeitung eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der betroffenen Personen (Gefahr im Verzug) vor, so kann die Datenschutzbehörde die Weiterführung der Datenverarbeitung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51/1991, untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenverarbeitung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Ebenso kann die Datenschutzbehörde auf Antrag einer betroffenen Person eine Einschränkung der Verarbeitung nach Art. 18 DSGVO mit Bescheid gemäß § 57 Abs. 1 AVG anordnen, wenn der Verantwortliche einer diesbezüglichen Verpflichtung nicht fristgerecht nachkommt. Wird einer Untersagung nicht unverzüglich Folge geleistet, hat die Datenschutzbehörde nach Art. 83 Abs. 5 DSGVO vorzugehen.

(5) Der Datenschutzbehörde obliegt im Rahmen ihrer Zuständigkeit die Verhängung von Geldbußen gegenüber natürlichen und juristischen Personen.

(6) Bestehen im Zuge einer auf § 29 gestützten Klage einer betroffenen Person, die sich von einer Einrichtung, Organisation oder Vereinigung im Sinne des Art. 80 Abs. 1 DSGVO vertreten lässt, Zweifel am Vorliegen der diesbezüglichen Kriterien, trifft die Datenschutzbehörde auf Antrag des Einbringungsgerichtes entsprechende Feststellungen mit Bescheid. Diese Einrichtung, Organisation oder Vereinigung hat im Verfahren Parteistellung. Gegen einen negativen Feststellungsbescheid steht ihr die Beschwerde an das Bundesverwaltungsgericht offen.



Verantwortliche des öffentlichen und des privaten Bereichs

DSG § 26. (1) Unbeschadet des § 5 Abs. 3 sind Verantwortliche des öffentlichen Bereichs sind alle Verantwortlichen,
1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.
(2) Verantwortliche des öffentlichen Bereichs sind Partei in Verfahren vor der Datenschutzbehörde.
(3) Verantwortliche des öffentlichen Bereichs können Beschwerde an das Bundesverwaltungsgericht und Revision beim Verwaltungsgerichtshof erheben.
(4) Die dem Abs. 1 nicht unterliegenden Verantwortlichen gelten als Verantwortliche des privaten Bereichs im Sinne dieses Bundesgesetzes.

Einrichtung

DSG § 18. (1) Die Datenschutzbehörde wird als nationale Aufsichtsbehörde gemäß Art. 51 DSGVO eingerichtet.
(2) Der Datenschutzbehörde steht ein Leiter vor. In seiner Abwesenheit leitet sein Stellvertreter die Datenschutzbehörde. Auf ihn finden die Regelungen hinsichtlich des Leiters der Datenschutzbehörde Anwendung.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen

DSG § 8. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adressdaten eines bestimmten Kreises von betroffenen Personen zum Zweck ihrer Benachrichtigung oder Befragung der Einwilligung der betroffenen Personen.

Anwendungsbereich und Durchführungsbestimmung

DSG § 4. (1) ...

(2) Kann die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt einzuschränken.

(3) Die Verarbeitung von personenbezogenen Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen ist unter Einhaltung der Vorgaben der DSGVO zulässig, wenn

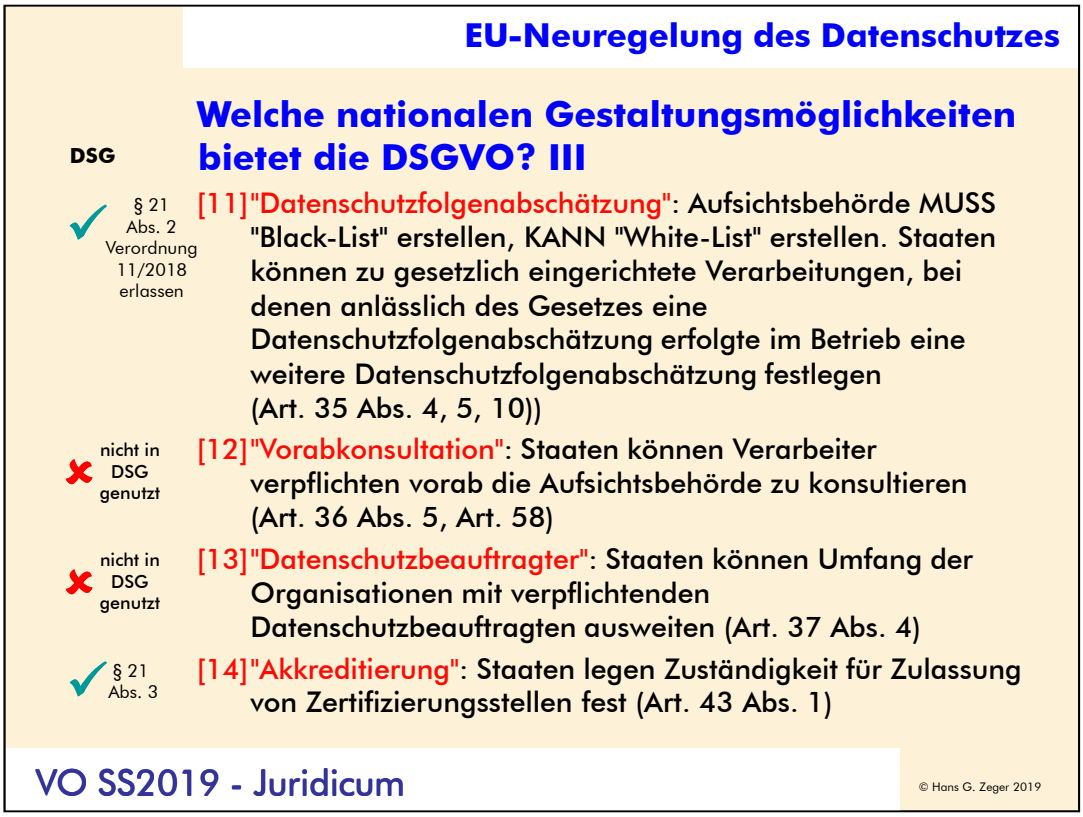
1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verarbeitung solcher Daten besteht oder
2. sich sonst die Zulässigkeit der Verarbeitung dieser Daten aus gesetzlichen Sorgfaltspflichten ergibt oder die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 lit. f DSGVO erforderlich ist, und die Art und Weise, in der die Datenverarbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person nach der DSGVO und diesem Bundesgesetz gewährleistet.

(4) Bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, ist die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO zur Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das vierzehnte Lebensjahr vollendet hat.

(5) Das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht gegenüber einem hoheitlich tätigen Verantwortlichen unbeschadet anderer gesetzlicher Beschränkungen dann nicht, wenn durch die Erteilung dieser Auskunft die Erfüllung einer dem Verantwortlichen gesetzlich übertragenen Aufgabe gefährdet wird.

(6) Das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO besteht gegenüber einem Verantwortlichen unbeschadet anderer gesetzlicher Beschränkungen in der Regel dann nicht, wenn durch die Erteilung dieser Auskunft ein Geschäfts- oder Betriebsgeheimnis des Verantwortlichen bzw. Dritter gefährdet würde.

(7) Soweit manuell, dh. nichtautomatisiert geführte Dateisysteme für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, gelten sie als Datenverarbeitungen im Sinne der DSGVO und dieses Bundesgesetzes.

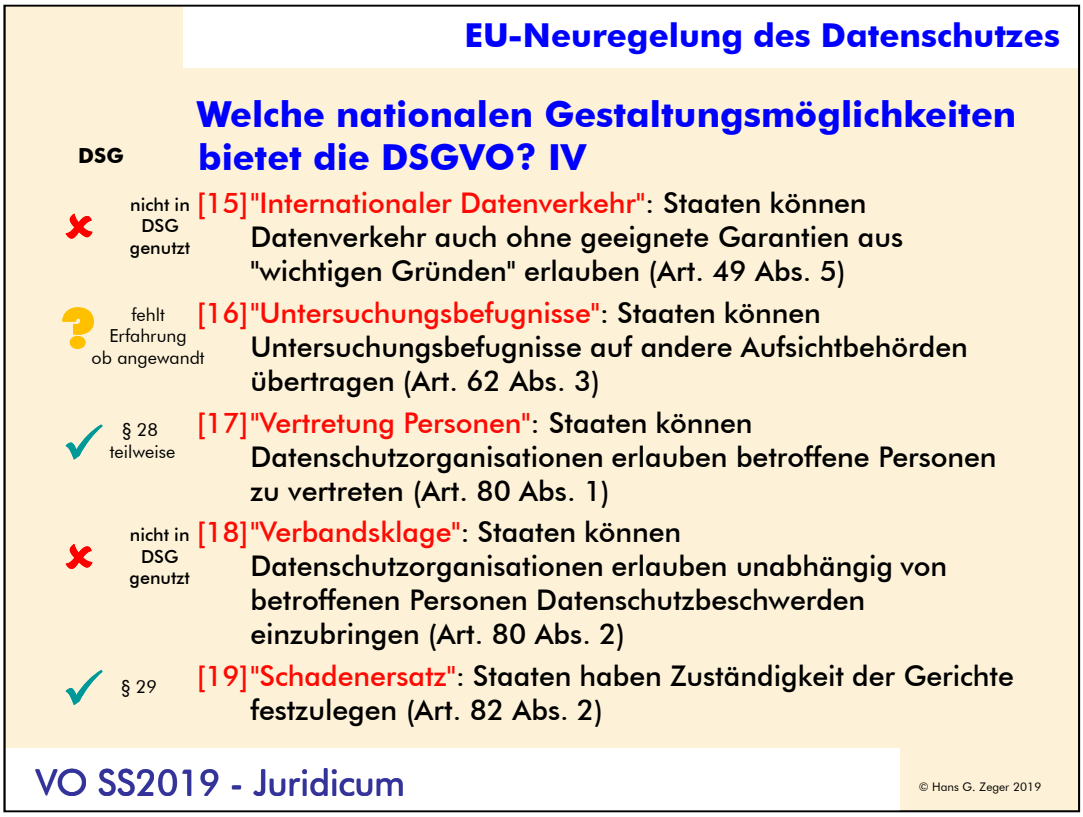


Aufgaben

DSG § 21. (1) Die Datenschutzbehörde berät die Ausschüsse des Nationalrates und des Bundesrates, die Bundesregierung und die Landesregierungen auf deren Ersuchen über legislative und administrative Maßnahmen. Die Datenschutzbehörde ist vor Erlassung von Bundesgesetzen sowie von Verordnungen im Vollzugsbereich des Bundes, die Fragen des Datenschutzes unmittelbar betreffen, anzuhören.

(2) Die Datenschutzbehörde hat die Listen nach Art. 35 Abs. 4 und 5 DSGVO im Wege einer Verordnung im Bundesgesetzblatt kundzumachen.

(3) Die Datenschutzbehörde hat die nach Art. 57 Abs. 1 lit. p DSGVO festzulegenden Kriterien im Wege einer Verordnung kundzumachen. Sie fungiert zugleich als einzige nationale Akkreditierungsstelle gemäß Art. 43 Abs. 1 lit. a DSGVO.



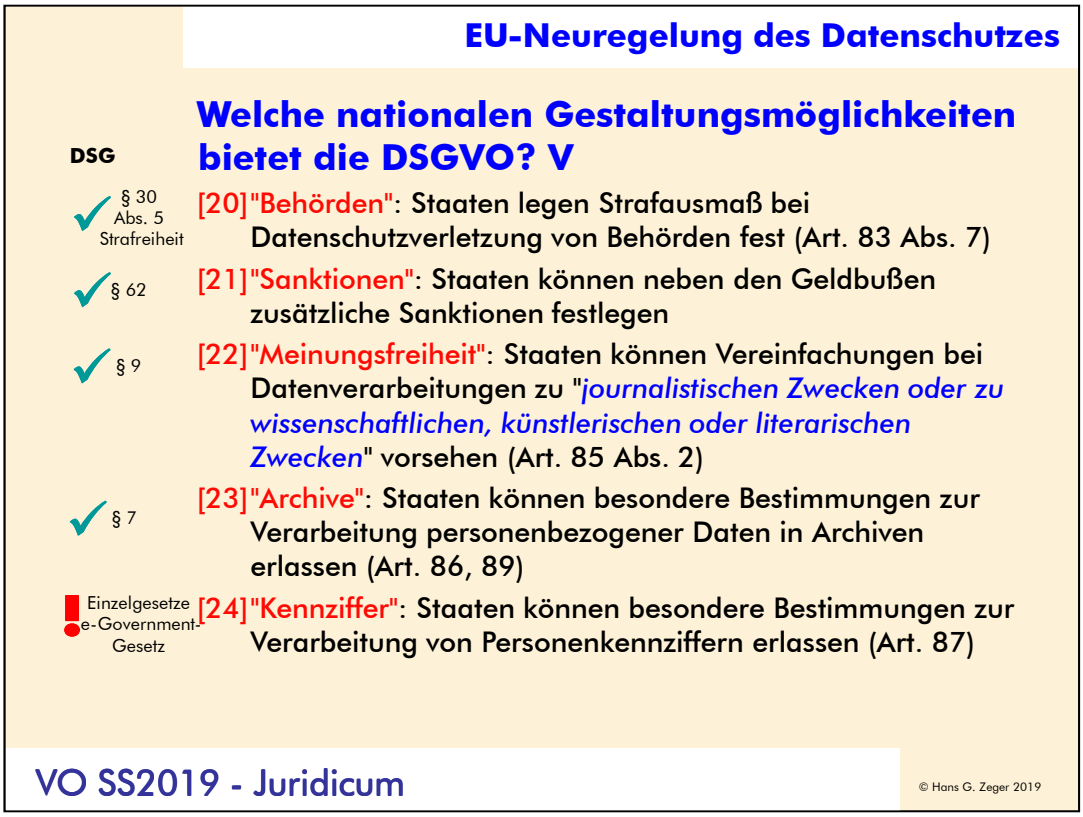
Vertretung von betroffenen Personen

DSG § 28. Die betroffene Person hat das Recht, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen und, in ihrem Namen die in den §§ 24 bis 27 genannten Rechte wahrzunehmen und das Recht auf Schadenersatz gemäß § 29 in Anspruch zu nehmen.

Haftung und Recht auf Schadenersatz

DSG § 29. (1) Jede Person, der wegen eines Verstoßes gegen die DSGVO oder gegen § 1 oder Artikel 2 1. Hauptstück ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter nach Art. 82 DSGVO. Im Einzelnen gelten für diesen Schadenersatzanspruch die allgemeinen Bestimmungen des bürgerlichen Rechts.

(2) Für Klagen auf Schadenersatz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat.



Allgemeine Bedingungen für die Verhängung von Geldbußen

DSG § 30. (1) Die Datenschutzbehörde kann Geldbußen gegen eine juristische Person verhängen, wenn Verstöße gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück durch Personen begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt haben und eine Führungsposition innerhalb der juristischen Person aufgrund

1. der Befugnis zur Vertretung der juristischen Person,

2. der Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder

3. einer Kontrollbefugnis innerhalb der juristischen Person

innehaben.

(2) Juristische Personen können wegen Verstößen gegen Bestimmungen der DSGVO und des § 1 oder Artikel 2 1. Hauptstück auch verantwortlich gemacht werden, wenn mangelnde Überwachung oder Kontrolle durch eine in Abs. 1 genannte Person die Begehung dieser Verstöße durch eine für die juristische Person tätige Person ermöglicht hat, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet.

(3) Die Datenschutzbehörde hat von der Bestrafung eines Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991 – VStG, BGBl. Nr. 52/1991, abzusehen, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird.

(4) ...

(5) Gegen Behörden und öffentliche Stellen, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, die im gesetzlichen Auftrag handeln, und gegen Körperschaften des öffentlichen Rechts können keine Geldbußen verhängt werden.

Welche nationalen Gestaltungsmöglichkeiten bietet die DSGVO? VI

DSG

✘ nicht in DSG genutzt

[25] "Beschäftigtendatenverarbeitung": Staaten können besondere Bestimmungen zum Beschäftigtendatenschutz erlassen (Art. 88)

✘ nicht in DSG genutzt

[26] "Verhaltensregeln": für Kirchen und Einrichtungen mit bestehenden umfassenden Datenschutzregelungen ("Verhaltensregeln") können spezifische Aufsichtsbehörden festgelegt werden (Art. 91)

✘ nicht in DSG genutzt

[27] "Verstorbene": DSGVO gilt nicht für verstorbene, Staaten können dazu jedoch Regeln verabschieden (EW27)

-

DSG - Anpassungen auf Grund der DSGVO

- ☺ Aufsichtsbehörde festgelegt (§ 18 DSG)
- ☹ Schutzalter gesenkt (§ 4 Abs. 4 DSG)
- ☺ private Einrichtungen dürfen notwendige Daten zu Straftaten verarbeiten [Whistleblowing, Strafregisterauszug MA] (§ 4 Abs. 3 DSG)
- 😐 Zuständigkeit für Akkreditierung geregelt (§ 21 Abs. 3 DSG)
- 😐 Datenschutzorganisationen dürfen Personen vertreten (§§ 23, 28 DSG)
- ☹ Behörden von Geldstrafen "befreit" (§ 30 Abs. 5 DSG)
- ☹ Informationsfreiheit und Archive geregelt (§§ 7, 9 DSG)

DSG - verpasste Chancen

- ✘ keine Regelung zum Arbeitnehmer-Datenschutz (Art. 88 DSGVO)
- ✘ keine Verbandsklagebefugnisse (Art. 80 DSGVO)
- ✘ keine Profiling-Regelungen (Art. 22 DSGVO)
- ✘ keine sinnvollen Sanktionen bei Behörden (Art. 83 DSGVO)
- ✘ keine generellen Vorgaben für Auftragsverarbeiter (Art. 28 DSGVO)

VO SS2019 - Juridicum

-

DSG - sonstige Regelungen

- 😐 Datenverwendung zu Verständigungszwecken (§ 8 DSG)
- 😐 Bildverarbeitung (§§ 12-13 DSG)

DSG - möglicherweise DSGVO/EU-widrig

- ✘ weiterhin existierender § 1 des DSG 2000
- ✘ Verarbeitungsbeschränkung statt Löschung (§ 4 Abs. 2 DSG)
- ✘ Beschränkung Auskunftsrecht bei "Gefährdung der Tätigkeit" oder bei "Gefährdung von Betriebsgeheimnissen" (§ 4 Abs. 5,6 DSG)
- ✘ zu weitreichende Ausnahmen im Zusammenhang mit Meinungsfreiheit (§ 9 DSG)
- ✘ Einflussnahme Gesetzgeber auf unabhängige Datenschutzbehörde ("Verwarnung" statt Strafe § 11 DSG)
- ✘ Fristsetzung bei Beschwerden (§ 24 Abs. 4 DSG)
- ✘ Ausdehnung der Straffreiheit auf private Unternehmen die im gesetzlichen Auftrag handeln (§ 30 Abs. 5 DSG)

-

Kontroll- & Strafbestimmungen

Welche Rechtsmittel / Sanktionen sind bei Verletzungen des Datenschutzes möglich?

- Unterlassungsanspruch
  - bei öffentlich-rechtlich tätigen Verantwortlichen (Behörden, ...): vor der Datenschutzbehörde (Entscheidungen jedoch nicht direkt durchsetzbar)
  - bei privat-rechtlich tätigen Verantwortlichern (Unternehmen, ...): Auskunftsfragen des Betroffenen (vor DSB, exekutierbar) alle anderen Fragen: vor den Zivilgerichten (LG)
- Schadenersatz
  - Ersatz materieller und "immaterieller" Schäden, Zivilgerichte (LG)
- strafrechtliche Verfolgung
- Verwaltungsübertretung
- unlauterer Wettbewerb (UWG)

VO SS2019 - Juridicum

-

Datenleck Heartbleed

Sicherheits-Vorfall

- Betreiber von Webseiten verwenden zur vertraulichen Kommunikation Verschlüsselung (Übertragung von Passwörtern, vertrauliche Kundendaten, VPN-Datenverkehr, ...)
- Verschlüsselungstechnik ist Transport Layer Security (TLS, auch als SSL bekannt)
- verwendete, weit verbreitete OpenSource Software openssl weist bei bestimmten Versionen (1.0.1*) eine Sicherheitslücke auf, die es Angreifern erlaubt, abgefangenen Datenverkehr zu entschlüsseln
- der Angriff kann erfolgen, ohne Spuren zu hinterlassen
- die Lücke existiert seit etwa zwei Jahren und wird erst jetzt bekannt

VO SS2019 - Juridicum

-

Datenleck Heartbleed

Verpflichtungen aus Sicht der Datensicherheit

- gemäß Art. 32 DSGVO sind Betreiber von Webseiten verpflichtet vertrauliche personenbezogene Daten angemessen zu sichern:
- DSGVO gibt nur wenige Hinweise, welche Maßnahmen konkret zu setzen sind (zB Hinweis auf Verschlüsselungsmöglichkeit, ...), GTelG verlangt jedoch bei Gesundheitsdaten ausdrücklich Verschlüsselung
- Verschlüsselung TLS entspricht - richtig konfiguriert - "Stand der Technik" und kann als geeignete Maßnahme zum Schutz gegen Zugriff Unbefugter angesehen werden
- Einsatz von openssl nach DSGVO zulässig und sinnvoll, Datenleck kann Betreiber nicht angelastet werden

⇨ **nach bekannt werden ist unverzügliches Handeln erforderlich!**

VO SS2019 - Juridicum

-

Datenleck Heartbleed

Verpflichtungen aus Sicht der Datensicherheit

- Prüfpflicht, ob betroffene Software installiert ist (trifft im Prinzip alle potentiell Betroffenen)
- wenn betroffen, unverzüglich Handeln:
  ⇨ Patch vorhanden: Installieren des Patches innerhalb weniger Stunden
  ⇨ kein Patch vorhanden: alternatives Produkt installieren oder Dienst vom Netz nehmen
- Informationspflicht der Betroffenen und der Aufsichtsstelle gemäß Art 33, 34 DSGVO + Hinweise welche persönliche Schutzmaßnahmen diese treffen können bzw. müssen, z.B. Passwortänderung
- wenn von Lücke nicht betroffen:
  Prüfpflicht ob eingesetzte Software vergleichbare Lücken aufweisen könnte. Diese Prüfpflicht kann auch an eigenen Softwarelieferant delegiert werden.

VO SS2019 - Juridicum

-

Sicherheitsmaßnahmen - Haftung

Haftung bei versuchtem Datenmissbrauch

OGH Entscheidung (9 Ob 126/12s)

Ausgangslage

Ein Redakteur der Tageszeitung A versuchte durch "erraten" von Benutzerkennung/Passwort im Zuge der BUWOG-Causa in das interne System des Unternehmens P zu gelangen.

Der Versuch misslang, auf Grund der IP-Adresse konnte der Standort des Täters ermittelt werden.

Die Aktion führte zur fristlosen Entlassung des Mitarbeiters.

Unternehmen P verlangt Unterlassungserklärung

Unternehmen P verlangt weiters von TZ A eine Unterlassungserklärung. Diese wird verweigert, da Redakteur nicht im Auftrag gehandelt habe, sich die TZ A von diesen Aktivitäten distanziere und daher der Redakteur nicht als Besorgungsgehilfe anzusehen ist.

VO SS2019 - Juridicum

OGH verschärft Haftung der Betriebe bei Datenmissbrauch 6 Ob 126/12s

OGH: Abhilfemöglichkeit des Arbeitgebers reicht für Verantwortung aus

Handle der unmittelbare Störer im Interesse oder im Verantwortungsbereich eines Dritten, so wäre dem Gestörten mit einem Anspruch bloß gegen den jederzeit austauschbaren unmittelbaren Störer wenig geholfen. Diese Überlegungen ließen sich auf den vorliegenden Fall übertragen. Die Beklagte habe den Computer mit der entsprechenden IP-Adresse zur Verfügung gestellt. Damit habe die Beklagte aber schon aufgrund dieses Umstands Einfluss auf Art und Weise der Benutzung dieses Anschlusses. Im Übrigen habe die Beklagte nach ihrem eigenen Vorbringen offenbar sogar direkte Durchgriffsrechte, hätte doch der Geschäftsführer der Beklagten den betreffenden Redakteur direkt suspendieren können.

Resumee - Haftung der Unternehmen auch ohne Schaden

Was auf den ersten Blick eher als skurriles Detail im Streit zwischen zwei Boulevardzeitungen anmutet, ist im Endeffekt ein wegweisendes Urteil. Die Haftung von Arbeitgebern für „Eigenaktionen“ einzelner Mitarbeiter wird damit wesentlich ausgeweitet.

Fehlende interne Sicherheits- und Kontrollmaßnahmen können bei Betrieben rasch zu hohen zivil- und strafrechtlichen Verpflichtungen führen.

Schon der Umstand, dass der Arbeitgeber sich seine Mitarbeiter aussuchen kann, ihnen die Arbeitsressourcen übergibt, ein Weisungs- und Kontrollrecht hat und die Mitarbeiter letztlich in seinem Interesse tätig werden, führt zu dessen Verantwortlichkeit für rechtswidrige Eingriffe. Dies ist auch zu begrüßen - ein Unterlassungsanspruch nur gegen den unmittelbaren Täter wäre hier so gut wie wirkungslos.

Abhilfe schafft in solchen Fällen nur ein wirksames internes Sicherheitssystem, dass derartige Fälle verhindert.

Haftung bei versuchtem Datenmissbrauch II

OGH Entscheidung (9 Ob 126/12s)

Entscheidung

HG gibt Klage statt, Vorinstanz (OLG) weist Klage ab, OGH gibt Klage statt, Eingriff ist nach Besitzstörung und nicht nach Schadenersatz zu beurteilen.

Eingriff in IT-System ist Besitzstörung

Eingriff war im Interesse der TZ A

Arbeitgeber hat Weisungs- und Kontrollrechte, kann sich Mitarbeiter aussuchen und Tätigkeitsbereich festlegen

Zur Verfügung stellen von Computer und Internetanschluss reicht schon für Verantwortung der TZ A

Unternehmen hat Besitzstörung - auch ohne ausdrückliche Anordnung - zu verantworten

-

Sicherheitsmaßnahmen - Haftung

Haftung bei fehlendem Zugriffsschutz

EGMR Entscheidung I. gegen Finnland (20511/03)
Sachverhalt:
Eine finnische Krankenschwester lässt sich im Spital in dem sie arbeitet wegen einer HIV-Infektion behandeln. Kurz darauf wird sie "gemobbt". Der Beweis, dass Personalführung rechtswidrig auf die Patientendaten zugegriffen hat misslingt.
Entscheidung des EGMR:
Es liegt trotzdem eine Verletzung des Grundrechts auf Privatsphäre vor (Art. 8 EMRK), da unzureichendes Sicherheitsmaßnahmen gesetzt waren.
Konsequenz:
Aus der Schutzverpflichtung erwächst die positive Pflicht, Personendaten effektiv und praktisch vor der Möglichkeit eines unautorisierten Zugriffs zu schützen; es reicht nicht aus, wenn dem Betroffenen eine Beschwerdemöglichkeit bei Datenmissbrauch gewährt wird

VO SS2019 - Juridicum

CASE OF I v. FINLAND (Application no. 20511/03):
JUDGMENT STRASBOURG 17 July 2008

...

37. The Court observes that it has not been contended before it that there was any deliberate unauthorised disclosure of the applicant's medical data such as to constitute an interference with her right to respect for her private life. Nor has the applicant challenged the fact of compilation and storage of her medical data. She complains rather that there was a failure on the part of the hospital to guarantee the security of her data against unauthorised access, or, in Convention terms, a breach of the State's positive obligation to secure respect for her private life by means of a system of data protection rules and safeguards. The Court will examine the case on that basis, having regard in particular to the fact that in the domestic proceedings the onus was on the applicant to prove the truth of her assertion.

38. The protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The above considerations are especially valid as regards protection of the confidentiality of information about a person's HIV infection, given the sensitive issues surrounding this disease. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (see Z v. Finland, judgment of 25 February 1997, Reports of Judgments and Decisions 1997-I, §§ 95-96).

...

Weitere Bestimmungen

- Privatsphäre-Bestimmung
- TelekommunikationsG 2003
- E-CommerceG
- sonstige Bestimmungen
- Weitere Entscheidungen/Beispiele

VO SS2019 - Juridicum

-

Schutz der Privatsphäre - § 1328a ABGB

§ 1328a ABGB Privatsphärebestimmung

(1) Wer rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingreift oder Umstände aus der Privatsphäre eines Menschen offenbart oder verwertet, hat ihm den dadurch entstandenen Schaden zu ersetzen. Bei erheblichen Verletzungen der Privatsphäre, etwa wenn Umstände daraus in einer Weise verwertet werden, die geeignet ist, den Menschen in der Öffentlichkeit bloßzustellen, umfasst der Ersatzanspruch auch eine Entschädigung für die erlittene persönliche Beeinträchtigung.

Abs.2 definiert Substitutionsklausel

- Bestimmung ist nicht anzuwenden, wenn andere Bestimmung gilt, etwa Datenschutz- oder Medienrechtsbestimmungen

VO SS2019 - Juridicum

§ 1328a Abs. 2 ABGB:

"(2) Abs. 1 ist nicht anzuwenden, sofern eine Verletzung der Privatsphäre nach besonderen Bestimmungen zu beurteilen ist. Die Verantwortung für Verletzungen der Privatsphäre durch Medien richtet sich allein nach den Bestimmungen des Mediengesetzes, BGBl. Nr. 341/1981, in der jeweils geltenden Fassung."

Schutz der Privatsphäre - § 1328a ABGB

Höhe des Schadenersatzes

- keine grundsätzliche Beschränkung der Entschädigungshöhe
- Orientierung am Medienrecht
- keine Untergrenze wie im ursprünglichen Entwurf vorgesehen

Ausnahmen

- Veröffentlichungen in Medien sind nicht erfasst (⇨ Mediengesetz)
- Betriebs- und Geschäftsgeheimnisse sind ausgenommen (⇨ §§ 122-124 StGB)
- speziellere Regelungen gehen vor (z.B. Art. 82 DSGVO)

VO SS2019 - Juridicum

Die Höhe der Entschädigung, die grundsätzlich zugesprochen werden kann ist nicht beschränkt, allerdings wird in den erläuternden Bemerkungen zum ursprünglichen Entwurf auf den §7 Abs. 1 Mediengesetz verwiesen, nach dem die Entschädigung einen Betrag von **EUR 20.000** nicht übersteigen darf. Da oft gerade Verletzungen der Privatsphäre durch Massenmedien besonders gravierend sind, ist anzunehmen, dass Entschädigungen nach dem §1328a kaum über dieser Grenze liegen werden.

Im ursprünglichen Entwurf war eine Untergrenze für die Entschädigung von EUR 1.000 vorgesehen. Diese wurde in die endgültige Fassung nicht übernommen. Die Untergrenze war im Vorfeld von einigen Experten kritisiert worden, weil dadurch u.U. die Situation entstehen hätte können, dass die Entschädigung höher als der tatsächliche Schaden ausfällt. Andererseits muss angemerkt werden, dass eine solche Untergrenze insbesondere in Fällen, in denen viele Personen gleichzeitig von einem Eingriff betroffen wären, zu einer besonders abschreckenden Wirkung geführt hätte, die solche Eingriffe bereits im Vorfeld verhindern hätte können.

Schutz der Privatsphäre - Beispiele

Beispiele für Eingriffe in die Privatsphäre

- private Videoüberwachung, Personenortung, Radarüberwachung
- Bekanntgabe persönlicher Daten im Internet
- Illegales Abhören von Telefonaten oder Gesprächen
- Hacken von privaten Computern
- Missbrauch von Foto-Handys
- Überwachung des Standortes eines Mobiltelefonnutzers ohne dessen Zustimmung
- Offenbaren/Verwerten von Urteilen
- **BG Josefstadt 6C188/09p** 8.7.2009 EV gemäß § 382g EO wegen Veröffentlichung privater Daten in einem Blog
  (begründet auf § 1328a ABGB "Cyberstalking")

VO SS2019 - Juridicum

Die oben genannten Beispiele sind teilweise auch in den erläuternden Bemerkungen zum Entwurf angeführt.

Es ist dazu allgemein anzumerken, dass sich der § 1328a ABGB auf den Ersatz immaterieller Schäden bezieht und insofern unabhängig von eventuell in anderen Gesetzen vorgesehenen (Verwaltungs-) Strafbestimmungen zu sehen ist.

So sind beispielsweise im TKG oder im DSG für verschiedene Tatbestände sowohl strafrechtliche als auch verwaltungsstrafrechtliche Sanktionen vorgesehen. Unabhängig von deren Anwendung könnten Betroffene bei entsprechendem Nachweis den Ersatz immaterieller Schäden verlangen.

elektronische Kommunikation und Datenschutz

Kommunikations-Rechtsrahmen der EU

- 2002 verabschiedet, 19.12.2009 geändert (2009/136/EG)
- in Ö durch TKG 2003 (BGBl I 70/2003) umgesetzt, Änderungen 21.11.2011 in (BGBl I 102/2011) umgesetzt
- wir beschränken uns auf 2002/58/EG und 2002/22/EG (Kommunikations-Datenschutz-RL & Universaldienst-RL) bzw. 12. Abschnitt des TKG 2003

Ziel der K-DS-RL war Regelung spezifischer Kommunikations-Datenschutzanforderungen und -situationen

- 2006 durch Vorratsdatenspeicherungsrichtlinie (2006/24/EG) ergänzt (in Ö 5/2011 umgesetzt, BGBl I 27+33/2011), 2014 vom EuGH wieder aufgehoben
- wichtigste Änderungen vom 19.12.2009/EG / 21.11.2011/TKG
  - Verständigungspflicht der Provider bei Datenverlust (2002/58/EG)
  - Ausschlußmöglichkeit von Urheberrechtsverletzern nach "unabhängigen" und "fairen" Verfahren (2002/22/EG)
  - Zustimmungspflicht bei "Cookie"-Einsatz (2002/58/EG)

VO SS2019 - Juridicum

Kommunikations-Rechtsrahmen der EU von 2002:

5 Richtlinien lösten alten Rechtsrahmen ab:

- Rahmenrichtlinie (2002/21/EG)
- Zugangsrichtlinie (Märkte, Marktbeherrschung, Trennung Infrastruktur/Geräte/Content) (2002/19/EG),
- Universaldienstrichtlinie (2003/22/EG)
- Genehmigungsrichtlinie (2002/20/EG)
- **Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG)**

Telekommunikationsgesetz 2003

Stammfassung BGBl. I Nr. 70/2003 (seit 20.08.2003), Novelle zur Vorratsdatenspeicehrung war im Mai 2007 in Begutachtung

Fernmeldegeheimnis (Art. 10a StGG)

seit 1.1.1975 als Gegenstück zum Briefgeheimnis (Art. 10 StGG)

elektronische Kommunikation und Datenschutz

Wer/Was fällt unter das TKG 2003? (§ 3 TKG 2003)

Betreiber(Bereitsteller/Anbieter) von Kommunikationsnetzen und/oder Kommunikationsdiensten

Kommunikationsnetz = Infrastruktur zur Übertragung von Signalen

Kommunikationsdienst = gewerbliche Dienstleistung mittels Übertragung von Signalen über Kommunikationsnetze

Betriebe, die auch Telefonvermittlungsanlagen betreiben oder Datenleitungen zur Vernetzung ihrer Standorte nutzen, fallen nicht darunter!

Einzelne Regeln betreffen alle Nutzer elektronischer Dienste z.B elektronische Werbung (§ 107), Löschungs-verpflichtung fehlerhaft zugestellter Nachrichten (§ 93 Abs. 4)

TKG 2003 regelt Datenschutzrechte der Benutzer (Nutzer/ Teilnehmer) gegenüber Betreibern (Bereitstellern/Anbietern)!

Neu mit Novelle 102/2011: Dienste der Informationsgesellschaft sind von Datenschutzregeln betroffen (§ 96 Abs. 3)

VO SS2019 - Juridicum

§ 3 ausgewählte Begriffe

Z1. -

2. „**Bereitsteller eines Kommunikationsnetzes**“ ein Unternehmen, das ein derartiges Netz errichtet, betreibt, kontrolliert oder zur Verfügung stellt;

Z9. "**Kommunikationsdienst**" eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben. Ausgenommen davon sind Dienste der Informationsgesellschaft im Sinne von § 1 Abs. 1 Z 2 des Notifikationsgesetzes, BGBl. I Nr. 183/1999, die nicht ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze bestehen;

Z11. "**Kommunikationsnetz**" Übertragungssysteme und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen, die die elektronische Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetze, feste (leitungs- und paketvermittelte, einschließlich Internet) und mobile terrestrische Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hörfunk und Fernsehen sowie Kabelrundfunknetze (Rundfunknetze), unabhängig von der Art der übertragenen Informationen;

Z14. "**Nutzer**" eine natürliche oder juristische Person, die einen öffentlich zugänglichen Kommunikationsdienst in Anspruch nimmt oder beantragt;

Z19. "**Teilnehmer**" eine natürliche oder juristische Person, die mit einem Betreiber einen Vertrag über die Bereitstellung dieser Dienste geschlossen hat;

§ 92. Abs 3 Definitionen zum Abschnitt "Kommunikationsgeheimnis, Datenschutz" (§§ 92-107)

Z1. "**Anbieter**" Betreiber von öffentlichen Kommunikationsdiensten;

Z2. "**Benutzer**" eine natürliche Person, die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben;

elektronische Kommunikation und Datenschutz

Vergleich TKG / DSG

TKG 2003	DSG
• RL 2002/58/EG	• DSGVO
• Stammdaten, Verkehrsdaten, Inhaltsdaten, Standortdaten	• alle personen-bezogenen Daten
• Betreiber iS TKG / Teilnehmer/Nutzer(Benutzer)	• alle Verantwortlicher / Betroffene
• Datensschutz-Bestimmungen §§ 92-107 + § 108 (Strafbestimmung)	• subsidiär anwendbar

VO SS2019 - Juridicum

-

TKG 2003 - Datenschutzbestimmungen

Geschützte Datenarten (§ 92 TKG 2003)

Stammdaten

Name, akademischer Grad, Anschrift, Teilnehmernummer, Konaktdaten, Vertragsdaten, Bonität, "öffentliche IP-Adresse" wenn Teilnehmer fix zugeordnet

Verkehrsdaten

z. B. Rufnummern, Datum, Zeit, Dauer, leistungsabhängige Entgelte, Funkzelle, inkl. "Zugangsdaten"

Inhaltsdaten

z. B. das geführte Telefonat, Fax, SMS, eMail-Inhalt, Webinhalte, ...

Standortdaten

genaue Position einer Kommunikationsendeinrichtung (kann bis auf wenige Meter genau bestimmt werden), im TKG nur für Kommunikationsnetze und -dienste definiert, nicht für Dienste der Informationsgesellschaft

VO SS2019 - Juridicum

TKG 2003 § 92 Abs 3 ...

3. „**Stammdaten**“ alle, auch personenbezogene Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

a) Name (Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen),

b) akademischer Grad bei natürlichen Personen,

c) Anschrift (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen),

d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,

e) Information über Art und Inhalt des Vertragsverhältnisses,

f) Bonität,

g) Geburtsdatum;

4. „**Verkehrsdaten**“ Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

4a. „**Zugangsdaten**“ jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind;

5. „**Inhaltsdaten**“ die Inhalte übertragener Nachrichten (Z 7);

6. „**Standortdaten**“ Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Telekommunikationsendeinrichtungen sind Standortdaten die Adresse der Einrichtung;

6a. „**Standortkennung**“ die Kennung einer Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird (Cell-ID);...

16.„**öffentliche IP-Adresse**“ eine einmalige numerische Adresse aus einem Adressblock, der durch die Internet Assigned Numbers Authority (IANA) oder durch eine regionale Vergabestelle (Regional Internet Registries) einem Anbieter eines Internet-Zugangsdienstes zur Zuteilung von Adressen an seine Kunden zugewiesen wurde, die einen Rechner im Internet eindeutig identifiziert und im Internet geroutet werden kann. Öffentliche IP-Adressen sind Zugangsdaten im Sinne des § 92 Abs. 3 Z 4a. Wenn eine konkrete öffentliche IP-Adresse einem Teilnehmer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 92 Abs. 3 Z 3;

TKG 2003 - Datenschutzbestimmungen

Stammdaten (§ 97 TKG 2003)

Name, akademischer Grad, Anschrift, Teilnehmernummer, Information über Art des Vertrags, Bonität, "öffentliche IP-Adresse" (unter bestimmten Umständen), Geburtsdatum

Verwendungszweck:

- Handhabung des Vertrages mit dem Teilnehmer
- Erstellung von Teilnehmerverzeichnissen
- Erteilung von Auskünften an Notrufträger

Löschungspflicht nach Beendigung der Rechtsbeziehungen!

[Weitreichender als bei sonstigen Verantwortlichern]

Ausnahmen: Entgeltverrechnung, laufende Beschwerden oder gesetzliche Verpflichtungen

VO SS2019 - Juridicum

§ 97. (1) Stammdaten dürfen unbeschadet der §§ 90 Abs. 6 und 7 sowie 96 Abs. 1 und 2 von Anbietern nur für folgende Zwecke ermittelt und verwendet werden:

1. Abschluss, Durchführung, Änderung oder Beendigung des Vertrages mit dem Teilnehmer;

2. Verrechnung der Entgelte;

3. Erstellung von Teilnehmerverzeichnissen, gemäß § 18 und

4. Erteilung von Auskünften an Notrufträger.

(1a) Vor Durchführung des Vertrages sowie vor der erstmaligen Wiederaufladung nach dem 1. September 2019 ist durch oder für den Anbieter die Identität des Teilnehmers zu erheben und sind die zur Identifizierung des Teilnehmers erforderlichen Stammdaten (§ 92 Abs. 3 Z 3 lit. a, b und g) anhand geeigneter Identifizierungsverfahren zu registrieren. Die Festlegung geeigneter Identifizierungsverfahren erfolgt durch Verordnung des Bundesministers für Verkehr, Innovation und Technologie im Einvernehmen mit dem Bundesminister für Inneres. Die Abgeltung unbedingt erforderlicher Investitionen erfolgt nach den Regeln des § 94 Abs. 1.

(2) Stammdaten sind spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.

TKG 2003 - Datenschutzbestimmungen

Verkehrsdaten (§ 99 TKG 2003)

besonders schutzwürdig

- „Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden“

grundsätzlich keine Speicherung, Ausnahmen:

- Verrechnung
- Entscheidung in Streitfällen – Übermittlung an die Schlichtungsstelle
- von 1.4.2012 bis 1.7.2014 Vorrats-Speicherpflicht für Überwachung bis 6 Monate - von EuGH und VfGH als grundrechtswidrig aufgehoben

ansonsten: keine starre Frist für die Speicherung

Auswertungsverbot

- zulässig für eine Vielzahl von Auskunftspflichten
- **aber:** kann durch Zustimmung des Teilnehmers für Marketingzwecke und Dienste mit Zusatznutzen erfolgen

VO SS2019 - Juridicum

§ 99. (1) Verkehrsdaten dürfen außer in den in diesem Gesetz geregelten Fällen nicht gespeichert oder übermittelt werden und sind vom Anbieter nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Die Zulässigkeit der weiteren Verarbeitung von Verkehrsdaten, die nach Abs. 5 übermittelt werden, richtet sich nach den Vorschriften der StPO, des FinStrG, des SPG sowie des PStSG.

...

(4) Dem Anbieter ist es außer in den in diesem Gesetz besonders geregelten Fällen untersagt, einen Teilnehmeranschluss über die Zwecke der Verrechnung hinaus nach den von diesem Anschluss aus angerufenen Teilnehmernummern auszuwerten. Mit Zustimmung des Teilnehmers darf der Anbieter die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen verwenden.

(5) Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist zulässig zur Auskunft über

1. Daten einer Nachrichtenübermittlung gemäß § 134 Z 2 StPO;

2. Zugangsdaten an Gerichte und Staatsanwaltschaften nach Maßgabe des § 76a Abs. 2 StPO.

3. Verkehrsdaten und Stammdaten, wenn hiefür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a und 3b SPG sowie § 11 Abs. 1 Z 5 PStSG. Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung verarbeitet werden;

4. Zugangsdaten, wenn diese längstens drei Monate vor der Anfrage gespeichert wurden, an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 3 SPG sowie § 11 Abs. 1 Z 5 PStSG;

5. Verkehrsdaten, Zugangsdaten und Standortdaten nach Maßgabe des § 11 Abs. 1 Z 7 PStSG.

TKG 2003 - Datenschutzbestimmungen

Inhaltsdaten (§ 101 TKG 2003)

Inhalte übertragener Nachrichten

keine Speicherung zulässig, außer wenn die Speicherung Dienstmerkmal ist (z. B. Mailbox)

Daten sind unverzüglich nach Diensterbringung vom Telekomanbieter/ISP zu löschen

VO SS2019 - Juridicum

§ 101. (1) Inhaltsdaten dürfen – sofern die Speicherung nicht einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt – grundsätzlich nicht gespeichert werden. Sofern aus technischen Gründen eine kurzfristige Speicherung erforderlich ist, hat der Anbieter nach Wegfall dieser Gründe die gespeicherten Daten unverzüglich zu löschen.

(2) Der Anbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass Inhaltsdaten nicht oder nur in dem aus technischen Gründen erforderlichen Mindestausmaß gespeichert werden. Sofern die Speicherung des Inhaltes Dienstmerkmal ist, sind die Daten unmittelbar nach der Erbringung des Dienstes zu löschen.

TKG 2003 - Datenschutzbestimmungen

Standortdaten (§ 102 TKG 2003)

Komplizierte Regelung „andere Standortdaten als Verkehrsdaten"
- Information über Funkzelle: Verkehrsdaten
- genauere Ortsangaben sind: „andere Standortdaten"

Verarbeitung nur
- anonymisiert (etwa zur Ressourcenplanung) oder
- mit jederzeit widerrufbarer Zustimmung des Betroffenen ("location based services")

muss auch zeitweise deaktivierbar sein

Datenart im Zusammenhang mit Anbietern von Kommunikationsdiensten im Sinne des TKG 2003 schwindende Bedeutung, da "location based services" meist über Drittanbieter ("Apps") erbracht werden

VO SS2019 - Juridicum

§ 102. (1) Andere Standortdaten als Verkehrsdaten dürfen unbeschadet des § 98 nur verarbeitet werden, wenn sie
1. anonymisiert werden oder
2. die Benutzer oder Teilnehmer eine jederzeit widerrufbare Einwilligung gegeben haben.

(2) Selbst im Falle einer Einwilligung zur Verarbeitung von Daten gemäß Abs. 1 müssen die Benutzer oder Teilnehmer die Möglichkeit haben, diese Verarbeitung von Daten für jede Übertragung einfach und kostenlos zeitweise zu untersagen.

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß Abs. 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln. Unbeschadet des § 93 Abs. 3 ist die Ermittlung und Verwendung von Standortdaten, die nicht im Zusammenhang mit einem Kommunikationsvorgang stehen, zu Auskunftszwecken unzulässig.

Kommunikationsdaten - Beispiel

Was ist ein Weblink / eine URL ?

- http://www.orf.at
- **https**://eservices.wuestenrot.at/eService/screen/anmeldung_ks210?_view=KS210_input_Komm&KS210_input_**Komm_auswei**s_art=RP&KS210_input_**Komm_ausw_nr**=4711&KS210_input_**Komm_ausw_b**ehoerde=BPD+Gossing&KS210_input_Komm_auswdat_tag=01&KS210_inpu t_Komm_auswdat_monat=01&KS210_input_Komm_auswdat_jahr=33&KS21 0_input_**Komm_handy**=0676+454545+&KS210_input_**Komm_email**=camp us%40gmx.at&KS210_input_**Komm_kennwort**=MANADA&KS210_input_Kom m_vertragsnr=&KS210_input_Komm_newsletter=0&checkAGB=true&KS210_ input_Komm_agb=on&KS210_input_Komm_KS210_input_Komm_forward= Weiter&_submit=true
- **Google-URL:**
  http://o-o.resolver.o.213.235.197.221.3d6303155122db29.l.google.com/
- **Newsletter-URL:**
  http://newsletter.avenum.com/app/include/ctr.php?ID=5O6619O128O214& email=hans.zeger@e-monitoring.at
  http://news.wko.at/sys/rd.aspx?sub=Q1PZGGK_30WCLYN&lnk=G4DT24B

VO SS2019 - Juridicum

-

TKG 2003 - Datenschutzbestimmungen

Kommunikationsgeheimnis (§ 93 TKG 2003)

schützt Inhaltsdaten, Verkehrsdaten und Standortdaten, inklusive erfolgloser Verbindungsversuche
[Stammdaten im Rahmen der DSGVO geschützt]

Verpflichtet Betreiber und deren Personal zur Geheimhaltung: gerichtliche Strafandrohung (§ 108 TKG 2003)

Mithören, Abfangen, Aufzeichnung oder sonstige Überwachen von Nachrichten durch andere als die Benutzer ist unzulässig (Zustimmung aller Beteiligten erforderlich), zufällig aufgenommene Nachrichten müssen gelöscht werden, gilt für alle "Anwender" (Abs. 4)

Ausnahmen (Abs. 3):
- Rückverfolgung von Notrufen
- Aufzeichnungen im Rahmen einer Fangschaltung
- Überwachung, Auskunftserteilung bei Nachrichtenübermittlung
- wenn technisch für Diensterbringung erforderlich (z.B. Mailbox)

VO SS2019 - Juridicum

§ 93. (1) Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Kommunikationsgeheimnisses ist jeder Betreiber eines öffentlichen Kommunikationsnetzes oder –dienstes und alle Personen, die an der Tätigkeit des Betreibers mitwirken, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung, der Überwachung von Nachrichten und der Auskunft über Daten einer Nachrichtenübermittlung sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.

(4) Werden mittels einer Funkanlage, einer Telekommunikationsendeinrichtung oder mittels einer sonstigen technischen Einrichtung Nachrichten unbeabsichtigt empfangen, die für diese Funkanlage, diese Telekommunikationsendeinrichtung oder den Anwender der sonstigen Einrichtung nicht bestimmt sind, so dürfen der Inhalt der Nachrichten sowie die Tatsache ihres Empfanges weder aufgezeichnet noch Unbefugten mitgeteilt oder für irgendwelche Zwecke verwertet werden. Aufgezeichnete Nachrichten sind zu löschen oder auf andere Art zu vernichten.

(5) Das Redaktionsgeheimnis (§ 31 Mediengesetz) sowie sonstige, in anderen Bundesgesetzen normierte Geheimhaltungsverpflichtungen sind nach Maßgabe des Schutzes der geistlichen Amtsverschwiegenheit und von Berufsgeheimnissen sowie das Verbot deren Umgehung gemäß §§ 144 und 157 Abs. 2 StPO zu beachten. Den Anbieter trifft keine entsprechende Prüfpflicht.

TKG 2003 - Datenschutzbestimmungen

Datenschutz-Grundsätze (§ 96 TKG 2003)

Verwendung der Daten nur für Zwecke der Besorgung eines Kommunikationsdienstes (Abs. 1)

Übermittlung (Abs. 2) nur, wenn
- notwendig für Diensterbringung oder
- mit Zustimmung des Betroffenen für Vermarktungszwecke oder Dienste mit Zusatznutzen (jederzeit widerrufbar)

Löschung (Abs. 2) der Daten sobald wie möglich
z. B.: Verkehrsdaten sind zu löschen, wenn für Dienst oder Abrechnung nicht mehr erforderlich

nähere Regelung der Datenverwendung in AGB möglich

VO SS2019 - Juridicum

§ 96. (1) Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten dürfen nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden.

(2) Die Übermittlung von im Abs. 1 genannten Daten darf nur erfolgen, soweit das für die Erbringung jenes Kommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, durch den Betreiber eines öffentlichen Kommunikationsdienstes erforderlich ist. Die Verwendung der Daten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen sowie sonstige Übermittlungen dürfen nur auf Grund einer jederzeit widerrufbaren Zustimmung der Betroffenen erfolgen. Diese Verwendung ist auf das erforderliche Maß und den zur Vermarktung erforderlichen Zeitraum zu beschränken. Betreiber öffentlicher Kommunikationsdienste dürfen die Bereitstellung ihrer Dienste nicht von einer solchen Zustimmung abhängig machen.

(3) **Betreiber öffentlicher Kommunikationsdienste und Anbieter eines Dienstes der Informationsgesellschaft im Sinne des § 3 Z 1 E-Commerce-Gesetz, BGBl. I Nr. 152/2001,** sind verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er verarbeiten wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Eine Ermittlung dieser Daten ist nur zulässig, wenn der Teilnehmer oder Nutzer seine Einwilligung dazu erteilt hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein Kommunikationsnetz ist oder, wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Benutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Der Teilnehmer ist auch über die Nutzungsmöglichkeiten auf Grund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen zu informieren. Diese Information hat in geeigneter Form, insbesondere im Rahmen Allgemeiner Geschäftsbedingungen und spätestens bei Beginn der Rechtsbeziehungen zu erfolgen. Das Auskunftsrecht nach dem Datenschutzgesetz und der DSGVO bleibt unberührt.

TKG 2003 - Datenschutzbestimmungen

Datenschutz-Grundsätze (§ 96 TKG 2003) II

Erweiterte Informations- und Zustimmungsverpflichtungen bei Diensterbringung (gelten für Betreiber öffentlicher Kommunikationsdienste und Anbieter eines Dienstes der Informationsgesellschaft (siehe ECG) (Abs. 3)

Informationspflichten:

- welche personenbezogene Daten Betreiber/Anbieter ermittelt, verarbeitet und übermittelt (betrifft auch Standort-/Geo-Daten)
- Rechtsgrundlage und Zweck der Datenverwendung
- Speicherdauer der Daten

Information ist in geeigneter Form, insbesondere mittels AGBs, spätestens bei Beginn einer Rechtsbeziehung zu erfolgen
[z.B. vor Setzen oder übermitteln von Cookies, ..]

VO SS2019 - Juridicum

-

TKG 2003 - Datenschutzbestimmungen

Datenschutz-Grundsätze (§ 96 TKG 2003) III

Abs. 3 - Fortsetzung

Ermittlung von Daten nur, wenn

- Teilnehmer oder Nutzer Einwilligung erteilt hat oder
- der alleinige Zweck die Übertragung einer Nachricht im Kommunikationsnetz ist oder
- wenn dies unbedingt erforderlich ist, damit ein Dienst der Informationsgesellschaft, den der Teilnehmer oder Benutzer ausdrücklich gewünscht hat erbracht werden kann
  [z.B. Session-Cookie für Online-Shop, GPS-Daten für location based services, ...]

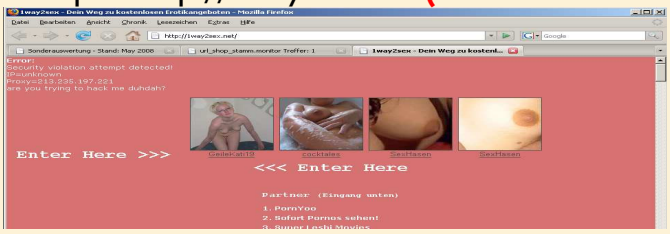
VO SS2019 - Juridicum

-

Demobeispiel Onlinetracking

Was passiert bei Aufruf einer Website?

Beispiel: http://1way2sex.net **(nicht mehr aktiv)**



Was wurde tatsächlich aufgerufen?

m1.webstats.motigo.com, vote4me.de, www.googleanalytics.com, www.toplistenservice.de, www.privatamateure.com, www.cyonix.to, ...

Betreiber dieser Server wurden vom Benutzer-Interesse an http://1way2sex.net informiert, kann vom Benutzer nicht beeinflusst werden

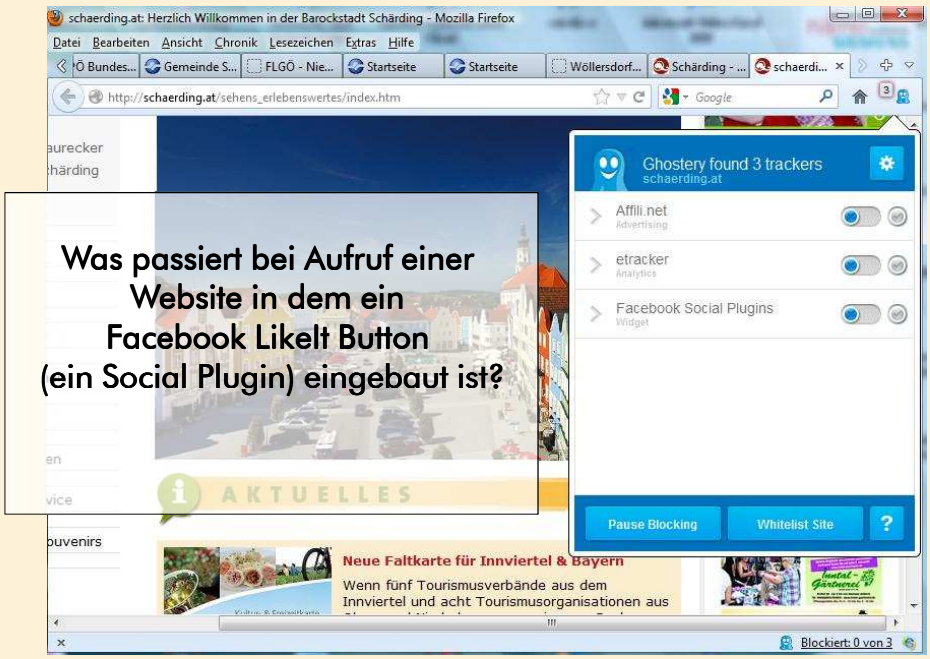
Zusatzinformation zu http://1way2sex.net:

Folgende Server setzen Cookies: (Auswahl, Stand 2009/06/04)

- 1way2sex.net
- activehitz.com
- www.ad-pay.de
- www.cash4images.info
- .cyonix.to
- www.deluxe-ads.net
- eas.apm.emediate.eu
- www.etracker.de
- www.fazfinance.net
- .funpic.de
- .hurra.com
- m1.webstats.motigo.com
- members.lycos.nl
- .overture.com
- www.privatamateure.com
- www.viking.de
- vote4me.de
- .webstats4u.com

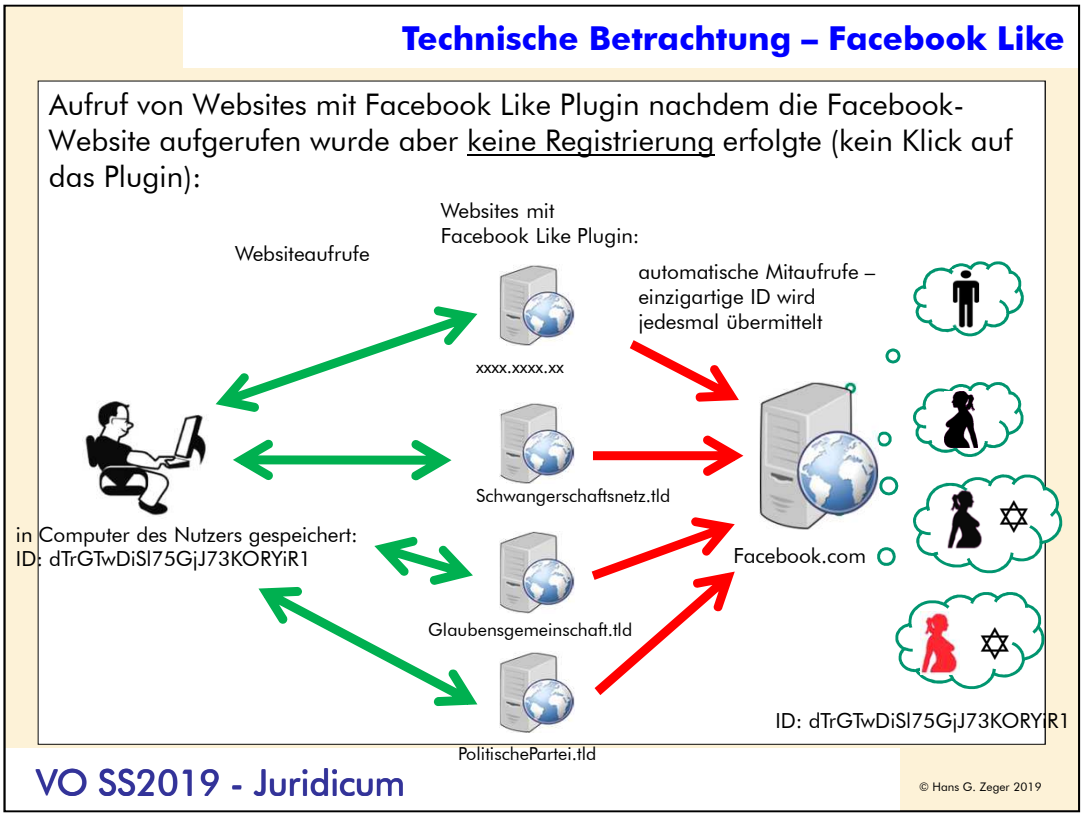
In Summe mehr als 20 Server/Organisationen

Facebook / LikeIt



VO SS2019 - Juridicum

-



Graphik: Michael Löffler, e-commerce monitoring Gmbh

Internet-Tracking in Österreich

Was ist eigentlich Tracking?

Der Begriff **Tracking** umfasst alle Bearbeitungsschritte, die der gleichzeitigen Verfolgung von (bewegten Personen dienen. ... Ziel dieser Verfolgung ist meist das Abbilder des beobachteten tatsächlichen Verhaltens zur technischen Verwertung. Solche Verwertung kann das Zusammenführen der *getrackten* Person mit bekannten Informationen sein. Solche Verwertung kann aber auch schlichter die jeweilige Kenntnis der tatsächlichen Identität der *getrackten* Person sein.

Identifizieren - Kombinieren - Verwerten sind offensichtlich die Ziele von Tracking

VO SS2019 - Juridicum

-

Internet-Tracking in Österreich

Welche Internet-Tracking-Formen kennen wir?

Cookies ✓	**bekannt, leicht zu unterbinden, schwach**
IP-Adresse ✓	**bekannt, oft irreführend (z.B. Internet-Cafes)**
MAC-Adressen ✓	**weniger bekannt, leicht zu manipulieren gut verwertbar**
Zählpixel ✓	**bekannt, vom Benutzer kaum abwehrbar, gut verwertbar**
Skripts, Plugins ✓	**bekannt, theoretisch leicht zu unterbinden, in der Praxis funktioniert dann "nichts" mehr, sehr effektiv**
Browser Toolbar ✓	**bewährt, erfordert Aktion des Benutzers, kann meist unauffällig installiert werden, extrem effektiv, wird nicht manipuliert**
persönliche Anmeldung ✓	**bewährt, erfordert jedoch schon Vertrags- oder zumindest Vertrauensbeziehung, sehr effektiv, letzte Stufe des Tracking**

VO SS2019 - Juridicum

-

Internet-Tracking in Österreich

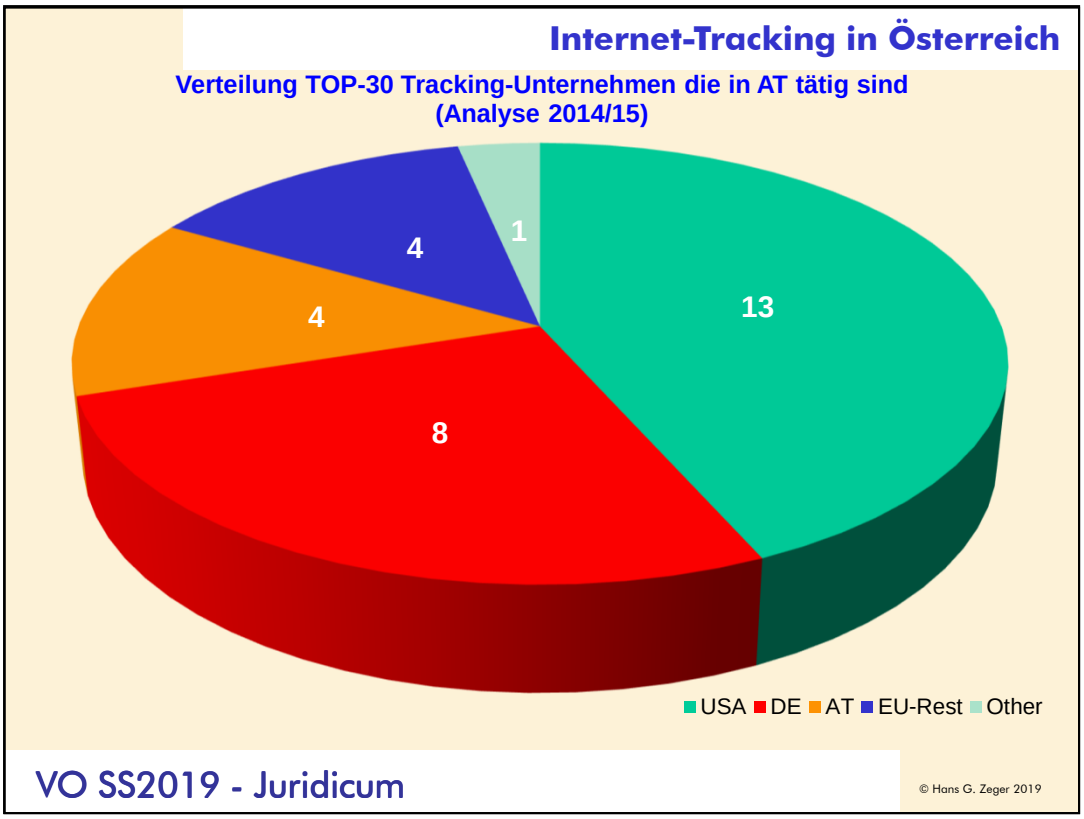
Welche Internet-Tracking-Formen kennen wir? II

Geräte-Signatur ✓	**bekannt, faktisch nicht manipulierbar, gut verwertbar und sehr effektiv**
Browserfont ✓	**weniger bekannt, nicht manipulierbar, sehr gut verwertbar und sehr effektiv**

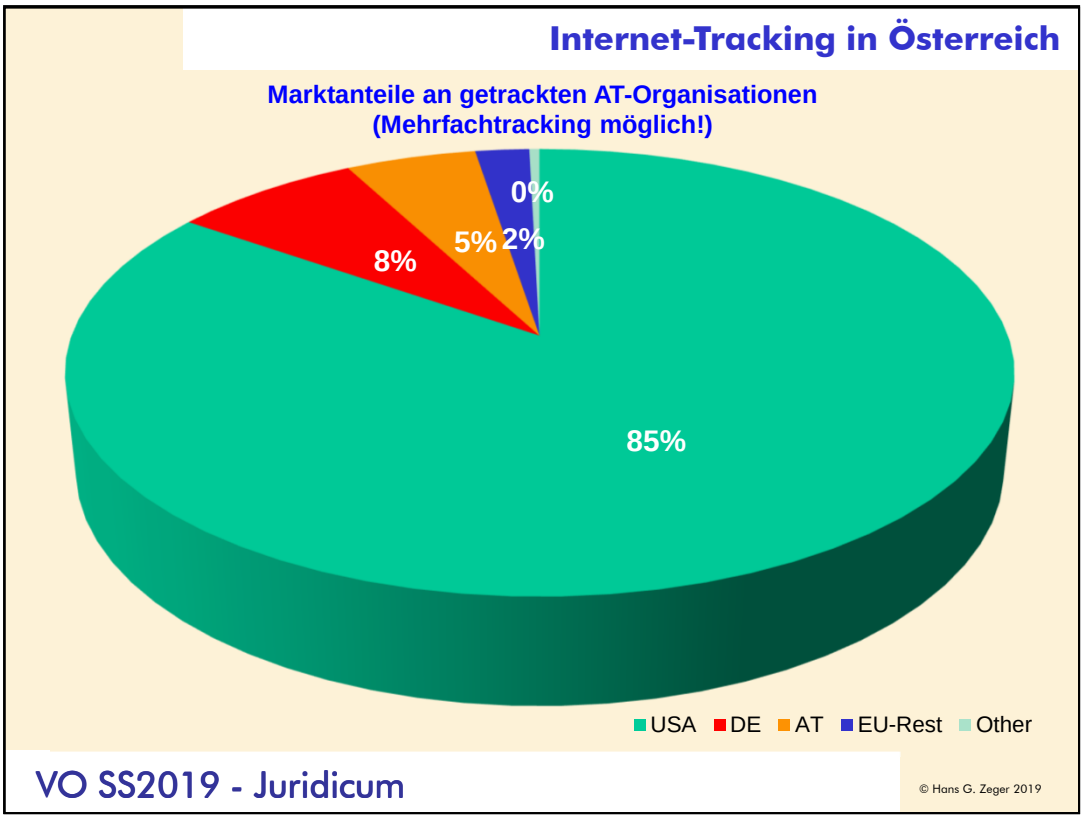
Der perfekte Tracker wird immer eine Kombination aller Techniken einsetzen!

VO SS2019 - Juridicum

-



Analysiert wurden die Webseiten von etwa 12.000 öffentlichen Einrichtungen und Unternehmen


Internet-Tracking in Österreich
Marktanteile an getrackten AT-Organisationen
(Mehrfachtracking möglich!)
0%
2%
5%
8%
85%
USA
DE
AT
EU-Rest
Other
VO SS2019 - Juridicum
© Hans G. Zeger 2019

-

Internet-Tracking in Österreich

Rechtlicher Rahmen?

Verwendet Tracking personenbezogene Daten?

DSGVO Art 4 Z 1 "personenbezogene Daten"
"alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen"

Datenbegriff sehr allgemein gehalten, umfasst
auch Bild- und Tondaten, biometrische Daten,
technische Kennzahlen
(z.B. IP-Adressen, Cookies, jede Art von Tracking-Daten, ...)

(technische) Möglichkeit der
Identifizierung einer Person reicht

VO SS2019 - Juridicum

-

Entscheidung Internet-Tracking - Frankreich

CNIL Beschwerde zweier Datenschutzorganisationen gegen Google 21.1.2019

Beschwerdegrund

- intransparente Datenschutzerklärung
- unzureichende Einwilligungsmöglichkeit

Ablauf

- CNIL kontaktierte andere EU-Datenschutzbehörden ("Konsultationsmechanismus")
- fand "keine Zuständigkeit", da Google keinen Hauptsitz in EU hat, sondern mehrere Sitze, irische DSB hatte keine ausreichenden Kapazitäten
- CNIL wurde auf nationaler Ebene aktiv
- Entscheidungsfindung erfolgte durch Online-Recherche einer Fachgruppe (erstellen von "Test-Accounts")

Auszug aus CNIL-Statement

https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

...

A violation of the obligation to have a legal basis for ads personalization processing:

The company GOOGLE states that it obtains the user's consent to process data for ads personalization purposes. However, the restricted committee considers that **the consent is not validly obtained for two reasons**.

First, the restricted committee observes that the users' consent is not sufficiently informed.

The information on processing operations for the ads personalization is diluted in several documents and does not enable the user to be aware of their extent. For example, in the section "Ads Personalization", it is not possible to be aware of the plurality of services, websites and applications involved in these processing operations (Google search, You tube, Google home, Google maps, Playstore, Google pictures…) and therefore of the amount of data processed and combined.

Then, the restricted committee observes that the collected consent is neither "specific" nor "unambiguous".

When an account is created, the user can admittedly modify some options associated to the account by clicking on the button « More options », accessible above the button « Create Account ». It is notably possible to configure the display of personalized ads.

That does not mean that the GDPR is respected. Indeed, the user not only has to click on the button "More options" to access the configuration, but the display of the ads personalization is moreover pre-ticked. However, as provided by the GDPR, consent is "unambiguous" only with a clear affirmative action from the user (by ticking a non-pre-ticked box for instance).

Finally, before creating an account, the user is asked to tick the boxes « *I agree to Google's Terms of Service*» and « *I agree to the processing of my information as described above and further explained in the Privacy Policy*» in order to create the account. Therefore, the user gives his or her consent in full, for all the processing operations purposes carried out by GOOGLE based on this consent (ads personalization, speech recognition, etc.). However, the GDPR provides that the consent is "specific" only if it is given distinctly for each purpose.

The fine imposed by the restricted committee and its publicity

The CNIL restricted committee publicly imposes a financial penalty of 50 Million euros against GOOGLE.

This is the first time that the CNIL applies the new sanction limits provided by the GDPR. The amount decided, and the publicity of the fine, are justified by the severity of the infringements observed regarding the essential principles of the GDPR: transparency, information and consent.

Despite the measures implemented by GOOGLE (documentation and configuration tools), the infringements observed deprive the users of essential guarantees regarding processing operations that can reveal important parts of their private life since they are based on a huge amount of data, a wide variety of services and almost unlimited possible combinations. The restricted committee recalls that the extent of these processing operations in question imposes to enable the users to control their data and therefore to sufficiently inform them and allow them to validly consent.

Moreover, the violations are continuous breaches of the Regulation as they are still observed to date. It is not a one-off, time-limited, infringement.

Finally, taking into account the important place that the operating system Android has on the French market, thousands of French people create, every day, a GOOGLE account when using their smartphone. Furthermore, the restricted committee points out that the economic model of the company is partly based on the ads personalization. Therefore, it is of its utmost responsibility to comply with the obligations on the matter.

Entscheidung Internet-Tracking - Frankreich II

Ergebnis der Prüfung

- Verletzung der Transparenz: Datenschutzinformation zB zum geo-tracking erst nach mehreren Schritten ("5-6 Aktionen") erreichbar
- Verletzung der Einwilligungserfordernis: Zustimmungsbox ist vorausgefüllt, zusätzlich muss der Nutzer mit einer Click-Box zahlreichen Funktionen zustimmen (ua "ads personalization, speech recognition, ...")

Entscheidung CNIL

- Beschwerden sind berechtigt
- Auf Grund der hohen Zahl betroffener französischer Nutzer wurde ine Strafe über 50 Mio Euro verhängt

Anmerkung(en)

- DSGVO-Konsultationsmechanismus noch nicht eingespielt
- hohe Bedeutung von Verbandsklagen (in Österreich nicht möglich)
- hohe Bedeutung eigener (technischer) Recherchen, statt Aktenverfahren
- Entscheidung kann als Orientierungshilfe zu Einwilligung und Transparenz angesehen werden und wird EU-Unternehmen binden

⇨ **Google wird die Entscheidung trotzdem "kalt" lassen**

-

Entscheidungen Internet-Tracking - Deutschland

Hanseatisches OLG 3 U 26/12 27.6.2013
Fehlende Datenschutzhinweise stellen Verstoß gegen UWG dar
(deutsche Normen: UWG §§ 3, 4 Nr. 11, 5, 8; TMG §§ 5, 13; HWG § 7 Abs. 1 Nr. 2)
vergleichbare österreichische Norm: § 96 TKG 2003

LG Hamburg 312 O 127/16 10.3.2016
Fehlende Aufklärung zu Google Analytics ist wettbewerbswidrig

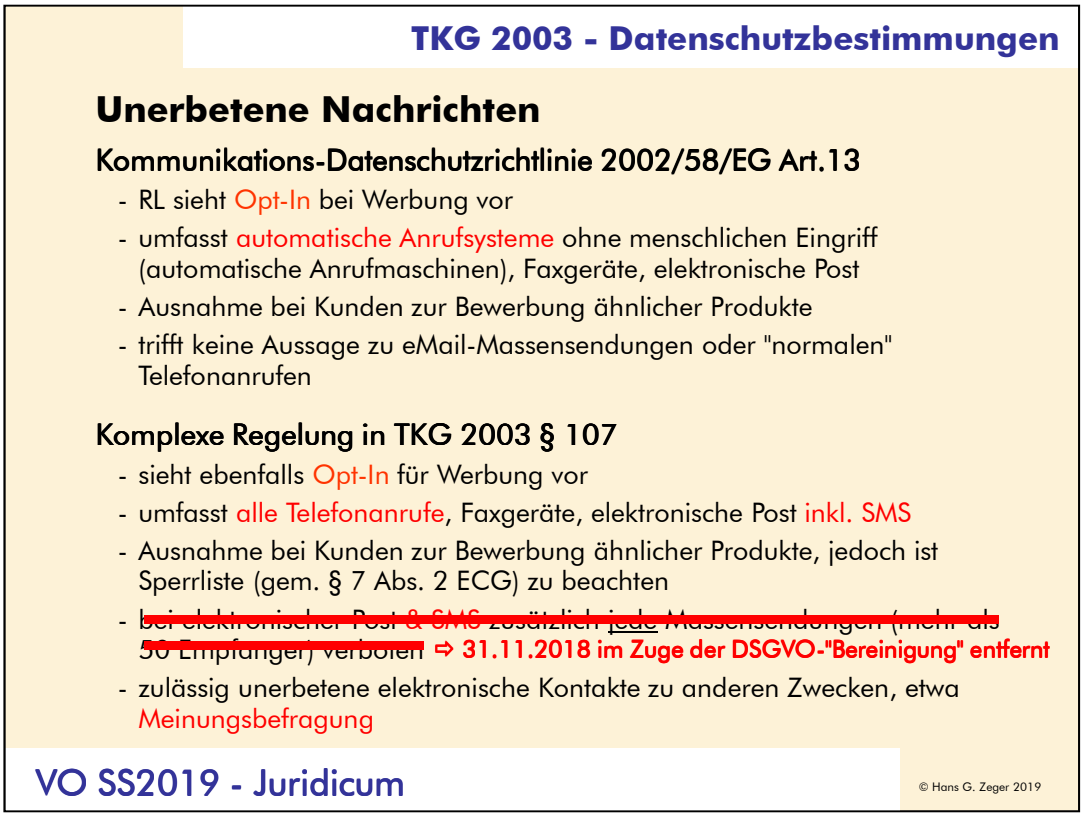
Vorgaben 2011 deutscher Datenschutzbehörden zu Google Analytics:
- DE-Webseitenbetreiber müssen Auftragsdatenverarbeitungsvertrag mit Google unterfertigen
- DE-Webseitenbetreiber müssen Benutzer über Einsatz aufklären und auf Widerspruchsmöglichkeit verweisen
- DE-Webseitenbetreiber müssen Google mit der Verkürzung der ermittelten IP-Adressen beauftragen

"Schon im Jahr 2011 haben die deutschen Datenschutzbehörden darüber informiert, wie aus ihrer Sicht ein zulässiger Einsatz des Analysetools auszusehen hat (Informationen der Datenschutzbehörde aus Hamburg):

- Webseitenbetreiber müssen den von Google vorbereiteten Vertrag zur Auftragsdatenverarbeitung schriftlich abschließen. Diesen Vertrag erhalten Sie unter „http://www.google.com/analytics/terms/de.pdf".
- Webseitenbetreiber müssen die Nutzer Ihrer Website in Ihrer Datenschutzerklärung über die Verarbeitung personenbezogener Daten im Rahmen von Google Analytics aufklären und auf die Widerspruchsmöglichkeiten gegen die Erfassung durch Google Analytics hinweisen. Hierbei sollte möglichst auf die entsprechende Seite „http://tools.google.com/dlpage/gaoptout?hl=de" verlinkt werden.
- Webseitenbetreiber müssen durch entsprechende Einstellungen im Google Analytics-Programmcode Google mit der Kürzung der IP-Adressen beauftragen. Dazu ist auf jeder Internetseite mit Analytics-Einbindung der Trackingcode um die Funktion „_anonymizeIp()" zu ergänzen.

Im konkreten Fall stellte der Webseitenbetreiber überhaupt keine Datenschutzerklärung und damit auch keine Informationen zum Einsatz von Google Analytics zur Verfügung. Damit lag ein Verstoß gegen die Informationspflicht des § 13 Abs. 1 S. 1 TMG vor. Bei dieser Vorschrift handelt es sich nach Auffassung vieler Gerichte (u.a. auch des OLG Hamburg, Urt. v. 27. Juni 2013 – Az. 3 U 26/12) um eine sogenannte Marktverhaltensregelung im Sinne des § 3a UWG. Die Verletzung einer solchen Regelung kann durch Wettbewerber abgemahnt und die Abgabe einer Unterlassungserklärung gefordert werden. Wenn eine solche Erklärung nicht rechtzeitig abgegeben wird, kann der Unterlassungsanspruch im Wege der einstweiligen Verfügung vor Gericht durchgesetzt werden, wie der oben verlinkte Beschluss einmal mehr zeigt."

aus https://www.delegedata.de/2016/03/landgericht-hamburg-untersagt-fehlerhaften-einsatz-von-google-analytics/ Stand 2016/05/07



Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) - *Artikel 13* Unerbetene Nachrichten

(1) Die Verwendung von automatischen Anrufsystemen ohne menschlichen Eingriff (automatische Anrufmaschinen), Faxgeräten oder elektronischer Post für die **Zwecke der Direktwerbung darf nur bei vorheriger Einwilligung** der Teilnehmer gestattet werden.

(2) Ungeachtet des Absatzes 1 kann eine natürliche oder juristische Person, wenn sie von ihren Kunden im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung gemäß der Richtlinie 95/46/EG deren elektronische Kontaktinformationen für elektronische Post erhalten hat, diese zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwenden, sofern die Kunden klar und deutlich die Möglichkeit erhalten, eine solche Nutzung ihrer elektronischen Kontaktinformationen bei deren Erhebung und bei jeder Übertragung gebührenfrei und problemlos abzulehnen, wenn der Kunde diese Nutzung nicht von vornherein abgelehnt hat.

TKG 2003 - Datenschutzbestimmungen

Unerbetene Nachrichten II

Regelung in TKG 2003 § 107

- Identität des Absenders muss offen gelegt werden
- Möglichkeit zur Einstellung der Zusendungen muss angeboten werden
- bei erlaubten Werbeanrufen, darf
  Anrufnummer weder unterdrückt, noch verfälscht sein,
  ECG-Bestimmungen nicht verletzt werden,
  nicht zum Besuch ECG-widriger Webseiten aufgefordert werden
- Anzeigemöglichkeit bei unerbetenen Nachrichten bei Fernmeldebüros
  (Verwaltungsstrafe bis 37.000 Euro bei Spam, 58.000 bei Anrufen),
  2012 (2011) 344 Anzeigen, 59 (35) Strafverfahren, Strafe Schnitt 196 (71) Euro
- Ort der "Tatbegehung" ist bei inländischen "Tätern" Sitz des Täters, bei anderen, der Ort an dem die Nachricht den Teilnehmer erreicht

Sonstige Maßnahmen gegen Spam

- anwaltliche Abmahnungen: Unterlassungsanspruch
- Spamfilter, Blocking-Listen und andere technische Maßnahmen: jedoch! Gefahr des Eingriffs in Kommunikation

Regelung gilt für alle, nicht nur Betreiber!

VO SS2019 - Juridicum

TKG 2003 § 107. (1) Anrufe - einschließlich das Senden von Fernkopien - zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers sind unzulässig. Der Einwilligung des Teilnehmers steht die Einwilligung einer Person, die vom Teilnehmer zur Benützung seines Anschlusses ermächtigt wurde, gleich. Die erteilte Einwilligung kann jederzeit widerrufen werden; der Widerruf der Einwilligung hat auf ein Vertragsverhältnis mit dem Adressaten der Einwilligung keinen Einfluss.

(1a) Bei Telefonanrufen zu Werbezwecken darf die Rufnummernanzeige durch den Anrufer nicht unterdrückt oder verfälscht werden und der Diensteanbieter nicht veranlasst werden, diese zu unterdrücken oder zu verfälschen.

(2) Die Zusendung einer elektronischen Post – einschließlich SMS – ist ohne vorherige Einwilligung des Empfängers unzulässig, wenn die Zusendung zu Zwecken der Direktwerbung erfolgt.

(3) Eine vorherige Einwilligung für die Zusendung elektronischer Post gemäß Abs. 2 ist dann nicht notwendig, wenn

1. der Absender die Kontaktinformation für die Nachricht im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und

2. diese Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und

3. der Empfänger klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung der elektronischen Kontaktinformation bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen und

4. der Empfänger die Zusendung nicht von vornherein, insbesondere nicht durch Eintragung in die in § 7 Abs. 2 E-Commerce-Gesetz genannte Liste, abgelehnt hat.

(Anm.: Abs. 4 aufgehoben durch BGBl. I Nr. 133/2005)

(5) Die Zusendung elektronischer Post zu Zwecken der Direktwerbung ist jedenfalls unzulässig, wenn

1. die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird, oder

2. die Bestimmungen des § 6 Abs. 1 E-Commerce-Gesetz verletzt werden, oder

3. der Empfänger aufgefordert wird, Websites zu besuchen, die gegen die genannte Bestimmung verstoßen oder

4. keine authentische Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.

(6) Wurden Verwaltungsübertretungen nach Absatz 1, 2 oder 5 nicht im Inland begangen, gelten sie als an jenem Ort begangen, an dem die unerbetene Nachricht den Anschluss des Teilnehmers erreicht.

TKG 2003 - Datenschutzbestimmungen

Sonstige Datenschutzbestimmungen im TKG

- Einrichtung und Betrieb technischer Überwachungsvorrichtungen (§ 94)
- Einzelentgeltnachweis (§ 100)
  kostenloser, elektronischer Einzelentgeltnachweis, auf Verlangen entgeltfrei in Papierform
- Telefonverzeichnis (§ 103)
  taxative Aufzählung der Datenarten, Verbot der Auswertung der Teilnehmerdaten (für den Anbieter)
- Anzeige der Rufnummer (§ 104)
- Unterdrückung des Versendens einer Rufnummer (§ 104)
- Anrufweiterleitung (§ 105)
- Fangschaltung (§ 106)

VO SS2019 - Juridicum

-

TKG 2003 - Datenschutzbestimmungen

Sicherheit im Netzbetrieb (§§ 95,95a TKG 2003)

2002/58/EG (Kommunikations-Datenschutz-RL, EG20, Art. 4)

- grundsätzliche Anforderung ähnlich der allg. DS-Richtlinie: angemessen, Stand der Technik, wirtschaftlich vertretbar
- in TKG § 95 Verweis auf DSGVO Art. 24, 25, 32

zusätzlich:

- Informationspflicht (§ 95a) des Nutzers/Teilnehmers bei Sicherheitsverletzung
- "doppelte" Informationspflicht bei Sicherheitsverletzung an Aufsichtsbehörde (RTR + Datenschutzbehörde)

Was ist Stand der Technik im Internet?

- im Zusammenhang mit Internet sind SSL128 (TSL, "https://") und VPN (Virtual Private Network) sind "Stand der Technik"

VO SS2019 - Juridicum

Datensicherheitsmaßnahmen

§ 95. (1) Die Pflicht zur Erlassung von Datensicherheitsmaßnahmen im Sinne der Art. 24, 25 und 32 DSGVO im Zusammenhang mit der Erbringung eines öffentlichen Kommunikationsdienstes obliegt jedem Betreiber eines öffentlichen Kommunikationsdienstes jeweils für jeden von ihm erbrachten Dienst.

(2) Unbeschadet des Abs. 1 hat der Betreiber eines öffentlichen Kommunikationsdienstes in jenen Fällen, in denen ein besonderes Risiko der Verletzung der Vertraulichkeit besteht, die Teilnehmer über dieses Risiko und – wenn das Risiko außerhalb des Anwendungsbereichs der vom Betreiber zu treffenden Maßnahmen liegt – über mögliche Abhilfen einschließlich deren Kosten zu unterrichten.

(3) Betreiber eines öffentlichen Kommunikationsdienstes haben – unbeschadet der Bestimmungen der DSGVO – durch Datensicherheitsmaßnahmen jedenfalls Folgendes zu gewährleisten:

1. die Sicherstellung, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten;
2. den Schutz gespeicherter oder übermittelter personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung oder Verarbeitung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe;
3. die Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten.

Die Regulierungsbehörde kann die von den Betreibern öffentlicher Kommunikationsdienste getroffenen Maßnahmen prüfen und Empfehlungen zum zu erreichenden Sicherheitsniveau abgeben.

Sicherheitsverletzungen

§ 95a. (1) Im Fall einer Verletzung des Schutzes personenbezogener Daten hat unbeschadet des § 16a sowie unbeschadet der Bestimmungen des Datenschutzgesetzes und der DSGVO der Betreiber öffentlicher Kommunikationsdienste unverzüglich die Datenschutzbehörde von dieser Verletzung zu benachrichtigen. Ist anzunehmen, dass durch eine solche Verletzung Personen in ihrer Privatsphäre oder die personenbezogenen Daten selbst beeinträchtigt werden, hat der Betreiber auch die betroffenen Personen unverzüglich von dieser Verletzung zu benachrichtigen.

(2) Der Betreiber öffentlicher Kommunikationsdienste kann von einer Benachrichtigung der betroffenen Personen absehen, wenn der Datenschutzbehörde nachgewiesen wird, dass er geeignete technische Schutzmaßnahmen im Sinne der Verordnung (EU) 611/2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG, ABl. Nr. L 173 vom 26.06.2013 S.2 (VO 611/2013) getroffen hat und dass diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewendet worden sind. Diese technischen Schutzmaßnahmen müssen jedenfalls sicherstellen, dass die Daten für unbefugte Personen nicht zugänglich sind.

(3) Unbeschadet der Verpflichtung des Betreibers nach Abs. 1 zweiter Satz kann die Datenschutzbehörde den Betreiber öffentlicher Kommunikationsdienste – nach Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung – auch auffordern, eine Benachrichtigung durchzuführen.

(4) Der Inhalt der Benachrichtigung der betroffenen Personen hat Art. 3 der VO 611/2013 zu entsprechen.

(5) Nähere Einzelheiten, insbesondere Form, Verfahrensweise oder Voraussetzungen für die Benachrichtigung bei einer Sicherheitsverletzung, kann der Bundeskanzler durch Verordnung festlegen. Die Datenschutzbehörde kann im Einzelfall auch entsprechende Anordnungen treffen, um eine den Auswirkungen der Sicherheitsverletzung angemessene Benachrichtigung der betroffenen Personen sicherzustellen. Sie kann auch Leitlinien im Zusammenhang mit Sicherheitsverletzungen erstellen.

(6) Die Betreiber öffentlicher Kommunikationsdienste haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen. Es hat Angaben zu den Umständen der Verletzungen, zu deren Auswirkungen und zu den ergriffenen Abhilfemaßnahmen zu enthalten und muss geeignet sein, der Datenschutzbehörde die Prüfung der Einhaltung der Bestimmungen gemäß Abs. 1 bis 4 zu ermöglichen.

(7) Die Datenschutzbehörde hat die Regulierungsbehörde über jene Sicherheitsverletzungen zu informieren, die für die Erfüllung der der Regulierungsbehörde durch § 16a übertragenen Aufgaben notwendig sind.

TKG 2003 - Datenschutzbestimmungen

Strafbestimmung TKG 2003 § 108
Verletzung von Rechten der Benützer

Strafandrohung für:

- Information an Unberufene über Tatsache und Inhalt eines Telekommunikationsverkehrs weitergibt (bzw. dazu Gelegenheit gibt, selbst wahrzunehmen)
- Nachricht fälscht, unrichtig wiedergibt, verändert, unterdrückt, unrichtig vermittelt oder unbefugt dem Empfangsberechtigten vorenthält
- Strafrahmen: Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen
- Täter ist nur auf Antrag des Verletzten zu verfolgen.
- **betrifft Betreiber und sein Pesonal (§ 93 Abs. 2)**
- Strafdrohungen für sonstige Nutzer von Kommunikationsdiensten in einem umfassenden Cybercrimepaket definiert (u.a. § 119 StGB)

VO SS2019 - Juridicum

TKG § 108 Verletzung von Rechten der Benützer

(1) Eine im § 93 Abs. 2 bezeichnete Person, die
1. unbefugt über die Tatsache oder den Inhalt des Telekommunikationsverkehrs bestimmter Personen einem Unberufenen Mitteilung macht oder ihm Gelegenheit gibt, Tatsachen, auf die sich die Pflicht zur Geheimhaltung erstreckt, selbst wahrzunehmen,
2. eine Nachricht fälscht, unrichtig wiedergibt, verändert, unterdrückt, unrichtig vermittelt oder unbefugt dem Empfangsberechtigten vorenthält,
ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen.

(2) Der Täter ist nur auf Antrag des Verletzten zu verfolgen.

§ 93 Abs. 2: "Zur Wahrung des Kommunikationsgeheimnisses ist jeder **Betreiber und alle Personen, die an der Tätigkeit des Betreibers mitwirken**, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist."

Cybercrime-Paket - Auszug

StGB § 118a Widerrechtlicher Zugriff auf ein Computersystem

StGB **§ 119 Verletzung des Telekommunikationsgeheimnisses**
(1) Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

StGB § 119a Missbräuchliches Abfangen von Daten

StGB § 120 Mißbrauch von Tonaufnahme- oder Abhörgeräten

Dienste der Informationsgesellschaft

Grundlagen Österreich

- E-Commerce-Gesetz – ECG, BGBl I 152/2001
  (unverändert seit 2001!)
- Fernabsatzgesetz, BGBl I 185/1999 (geregelt im KSchG)
  ab 13. Juni 2014 Verbraucherrechte-Richtlinie-Umsetzungsgesetz – VRUG, BGBl I 33/2014
- Mediengesetz, BGBl I 49/2005, 151/2005
- Handelsrechts-Änderungsgesetz – HaRÄG, BGBl I 120/2005
  (geregelt im Unternehmensgesetzbuch)

Grundlagen EU

- EG-Richtlinie 2000/31/EG "Richtlinie über den elektronischen Geschäftsverkehr"

Regelung

- regeln diverse Informations- und Auskunftspflichten bei Onlinediensten gem NotifG 1999 § 1 Abs 1 Z 2

VO SS2019 - Juridicum

Anwendungsbereich

Die EU-Richtlinien gelten nur für den Binnenmarkt, österreichische Konsumentenschutzbestimmungen könnten auch gegenüber Nicht-EU-Anbieter angewandt werden (sofern sich das Angebot ausdrücklich an österreichische Konsumenten wendet).

BGBl. I Nr. 183/1999 (StF) - Notifikationsgesetz 1999 - NotifG 1999

§ 1. (1) Im Sinne dieses Bundesgesetzes bedeuten:

...

2. „Dienst": eine Dienstleistung der Informationsgesellschaft, das ist jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, wobei im Sinne dieser Definition bedeuten:

a) „im Fernabsatz erbrachte Dienstleistung": eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Parteien erbracht wird,

b) „elektronisch erbrachte Dienstleistung": eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung, einschließlich digitaler Kompression, und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen und vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischen Weg gesendet, weitergeleitet und empfangen wird, und

c) „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung": eine Dienstleistung, die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird;

Anlage 1 enthält eine nicht abschließende Liste jener Dienstleistungen, die nicht unter diese Definition fallen;

E-Commerce-Gesetz

Geltungsbereich §§ 1ff ECG

- geregelt wird elektronischer Geschäfts- und Rechtsverkehr
- Zulassung von Diensteanbietern, Informationspflichten, Abschluss von Verträgen, Verantwortlichkeit von Diensteanbietern (§ 1)
- von den Bestimmungen unberührt bleiben Belange des Abgabenwesens, des Datenschutzes und des Kartellrechts (§ 2)
- **Dienst der Informationsgesellschaft (§ 3 Z 1):** elektronisch im Fernabsatz auf individuellen Abruf des Empfängers (in der Regel) gegen Entgelt bereitgestellter Dienst, insbesondere
  - Online-Vertrieb von Waren und Dienstleistungen,
  - Online-Informationsangebote,
  - Online-Werbung,
  - elektronische Suchmaschinen,
  - Datenabfragemöglichkeiten,
  - Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern (Access-, eMail-Dienste)

VO SS2019 - Juridicum

§ 1 ECG (1) Dieses Bundesgesetz regelt einen rechtlichen Rahmen für bestimmte Aspekte des elektronischen Geschäfts- und Rechtsverkehrs. Es behandelt die Zulassung von Diensteanbietern, deren Informationspflichten, den Abschluss von Verträgen, die Verantwortlichkeit von Diensteanbietern, das Herkunftslandprinzip und die Zusammenarbeit mit anderen Mitgliedstaaten im elektronischen Geschäfts und Rechtsverkehr.

(2) Die Bestimmungen dieses Bundesgesetzes über das Herkunftslandprinzip (§§ 20 bis 23) und die Zusammenarbeit mit anderen Mitgliedstaaten (§ 25) sind nur auf den Verkehr von Diensten der Informationsgesellschaft innerhalb des Europäischen Wirtschaftsraums anzuwenden.

§ 2. Dieses Bundesgesetz lässt Belange des Abgabenwesens, des Datenschutzes und des Kartellrechts unberührt.

§ 3. Im Sinne dieses Bundesgesetzes bedeuten:

1. **Dienst der Informationsgesellschaft:** ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst (§ 1 Abs. 1 Z 2 Notifikationsgesetz 1999), insbesondere der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern;

E-Commerce-Gesetz

Geltungsbereich §§ 1ff ECG II

- **Diensteanbieter (§ 3 Z 2):** eine natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die einen Dienst der Informationsgesellschaft bereitstellt
- **Nutzer (§ 3 Z 3):** nimmt Dienst in Anspruch
- **Verbraucher (§ 3 Z 4):** natürliche Person, die zu Zwecken handelt, die nicht zu ihren gewerblichen, geschäftlichen oder beruflichen Tätigkeiten gehören

OGH 4Ob219/03i 1.6.2005 ("Online-Sexdienste")

- Angeboten wurde Dialerzugang zu Porno-Webcams, geklagt wurde mangelnde Auszeichnung gem. ECG

Entscheidung

- Dienst im Sinne § 3 Z 1 ECG liegt bei Datenübertragung im Weg einer bidirektionalen Punkt-zu-Punkt-Verbindung vor
- Nutzer kann Dienst interaktiv nach seinen Bedürfnissen (zB betreffend Zeit und Ort der Nutzung sowie Art des abgerufenen Inhalts) steuern
- trifft auf Live-Cam-Darbietungen zu

VO SS2019 - Juridicum

§ 3 ECG ...

2. **Diensteanbieter:** eine natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die einen Dienst der Informationsgesellschaft bereitstellt;

3. **niedergelassener Diensteanbieter:** ein Diensteanbieter, der eine Wirtschaftstätigkeit mittels einer festen Einrichtung auf unbestimmte Zeit tatsächlich ausübt, wobei das Vorhandensein und die Nutzung von technischen Mitteln und Technologien, die zur Bereitstellung des Dienstes erforderlich sind, für sich allein noch keine Niederlassung des Diensteanbieters begründen;

4. **Nutzer:** eine natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die zu beruflichen oder sonstigen Zwecken einen Dienst der Informationsgesellschaft in Anspruch nimmt, insbesondere um Informationen zu erlangen oder Informationen zugänglich zu machen;

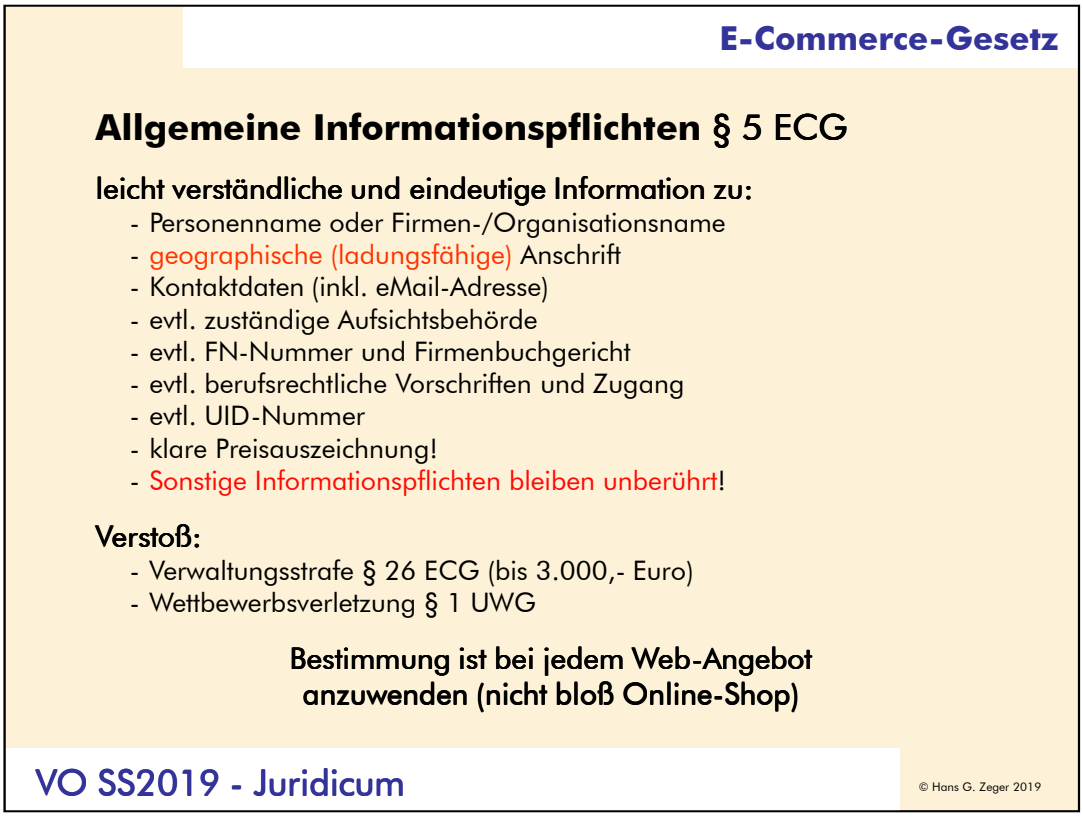
5. **Verbraucher:** eine natürliche Person, die zu Zwecken handelt, die nicht zu ihren gewerblichen, geschäftlichen oder beruflichen Tätigkeiten gehören;

6. **kommerzielle Kommunikation:** Werbung und andere Formen der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren und Dienstleistungen oder des Erscheinungsbildes eines Unternehmens dienen, ausgenommen

a) Angaben, die einen direkten Zugang zur Tätigkeit des Unternehmens ermöglichen, etwa ein Domain-Name oder eine elektronische Postadresse, sowie

b) unabhängig und insbesondere ohne finanzielle Gegenleistung gemachte Angaben über Waren, Dienstleistungen oder das Erscheinungsbild eines Unternehmens;

7. **Mitgliedstaat:** ein Mitgliedstaat der Europäischen Gemeinschaft oder des Abkommens über den Europäischen Wirtschaftsraum;



Informationspflichten Allgemeine Informationen

§ 5. (1) Ein Diensteanbieter hat den Nutzern ständig zumindest folgende Informationen leicht und unmittelbar zugänglich zur Verfügung zu stellen:

1. seinen Namen oder seine Firma;

2. die geografische Anschrift, unter der er niedergelassen ist;

3. Angaben, auf Grund deren die Nutzer mit ihm rasch und unmittelbar in Verbindung treten können, einschließlich seiner elektronischen Postadresse;

4. sofern vorhanden, die Firmenbuchnummer und das Firmenbuchgericht;

5. soweit die Tätigkeit einer behördlichen Aufsicht unterliegt, die für ihn zuständige Aufsichtsbehörde;

6. bei einem Diensteanbieter, der gewerbe- oder berufsrechtlichen Vorschriften unterliegt, die

Kammer, den Berufsverband oder eine ähnliche Einrichtung, der er angehört, die Berufsbezeichnung und den Mitgliedstaat, in dem diese verliehen worden ist, sowie einen Hinweis auf die anwendbaren gewerbe- oder berufsrechtlichen Vorschriften und den Zugang zu diesen;

7. sofern vorhanden, die Umsatzsteuer-Identifikationsnummer.

(2) Sofern in Diensten der Informationsgesellschaft Preise angeführt werden, sind diese so auszuzeichnen, dass sie ein durchschnittlich aufmerksamer Betrachter leicht lesen und zuordnen kann. Es muss eindeutig erkennbar sein, ob die Preise einschließlich der Umsatzsteuer sowie aller sonstigen Abgaben und Zuschläge ausgezeichnet sind (Bruttopreise) oder nicht. Darüber hinaus ist auch anzugeben, ob Versandkosten enthalten sind.

(3) Sonstige Informationspflichten bleiben unberührt.

E-Commerce-Gesetz

sonstige spezifische Diensteanbieter
(§§ 13-17 ECG)

- **Durchleitung von Informationen (§ 13) ("AccessProvider")** umfasst auch kurzfristiges Zwischenspeichern, etwa eMail für die Dauer der Diensterbringung
- **Suchmaschinenbetreiber (§ 14)**
- **Caching- und Proxy-Dienste (§ 15)**
- **Hosting-Dienste (§ 16) ("Hosting-Provider")**
  umfasst Bereitstellung von Speicherplatz für Webseiten, Blogs, Gästebücher, Diskussionsforen, Social Media Plattformen (z.B. Facebook), aber auch nicht-öffentliche Datenbestände
- **Link-Dienste (§ 17)**
  Bereitstellen eines Informationszugangs durch Links

VO SS2019 - Juridicum

-

e-commerce - Diensteanbieter

Verantwortung spezifischer Diensteanbieter
(§§ 13-14 ECG)

- Durchleitung von Informationen (§ 13) ("AccessProvider")
  Definition umfasst auch technisch erforderliches Zwischenspeichern, etwa eMail
- Suchmaschinen (§ 14)

Keine Verantwortung unter bestimmten Umständen:

1. die Übermittlung/Abfrage nicht veranlasst,
2. den Empfänger der übermittelten/abgefragten Informationen nicht auswählt
   und
3. die übermittelten/abgefragten Informationen weder auswählt noch verändert.

Auskunftspflicht im Fall § 13 gegenüber Gerichten zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen

VO SS2019 - Juridicum

Ausschluss der Verantwortlichkeit bei Durchleitung

§ 13. (1) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt oder den Zugang zu einem Kommunikationsnetz vermittelt, ist für die übermittelten Informationen nicht verantwortlich, sofern er
1. die Übermittlung nicht veranlasst,
2. den Empfänger der übermittelten Informationen nicht auswählt und
3. die übermittelten Informationen weder auswählt noch verändert.

(2) Die Übermittlung von Informationen und die Vermittlung des Zugangs im Sinn des Abs. 1 umfassen auch die automatische kurzzeitige Zwischenspeicherung der übermittelten Informationen, soweit diese Zwischenspeicherung nur der Durchführung der Übermittlung im Kommunikationsnetz dient und die Information nicht länger gespeichert wird, als es für die Übermittlung üblicherweise erforderlich ist.

Ausschluss der Verantwortlichkeit bei Suchmaschinen

§ 14. (1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er
1. die Übermittlung der abgefragten Informationen nicht veranlasst,
2. den Empfänger der abgefragten Informationen nicht auswählt und
3. die abgefragten Informationen weder auswählt noch verändert.

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird

e-commerce - Diensteanbieter

Verantwortung spezifischer Diensteanbieter II
(§ 15 ECG)

- Zwischenspeicherung (Caching) von Informationen (§ 15)

Keine Verantwortung unter bestimmten Umständen:

1. Keine Änderung der Information,
2. Bedingungen zum Informationszugang werden beachtet [z.B. kein allgemein zugänglich machen gesperrter Information],
3. Aktualisierung gemäß "Industriestandard" (?!),
4. Technologien zum Sammeln von Informationen lt. "Industriestandard" dürfen nicht beeinträchtigt werden (??) und
5. Unverzügliches entfernen der Information, wenn am Ursprungsort nicht vorhanden oder Gericht/Verwaltungsbehörde Sperre/Entfernung angeordnet hat

VO SS2019 - Juridicum

Ausschluss der Verantwortlichkeit bei Zwischenspeicherungen (Caching)

§ 15. Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt, ist für eine automatische, zeitlich begrenzte Zwischenspeicherung, die nur der effizienteren Gestaltung der auf Abruf anderer Nutzer erfolgenden Informationsübermittlung dient, nicht verantwortlich, sofern er

1. die Information nicht verändert,
2. die Bedingungen für den Zugang zur Information beachtet,
3. die Regeln für die Aktualisierung der Information, die in allgemein anerkannten und verwendeten Industriestandards festgelegt sind, beachtet,
4. die zulässige Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in allgemein anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigt und
5. unverzüglich eine von ihm gespeicherte Information entfernt oder den Zugang zu ihr sperrt, sobald er tatsächliche Kenntnis davon erhalten hat, dass die Information am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt oder der Zugang zu ihr gesperrt wurde oder dass ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperre angeordnet hat.

e-commerce - Diensteanbieter

Verantwortung spezifischer Diensteanbieter III
(§§ 16-17 ECG)

- Hosting / Housing von Diensten (§ 16)
  Auftragsverarbeiter speichert vom Nutzer eingegebene Daten
  - Unternehmenswebsite wird auf Server eines ISP verwaltet
  - Online-Händler mietet sich auf Webshop-Plattform ein
  - Leser gibt Kommentar in Onlineforum einer Zeitung ab
  - Benutzer bewertet Hotel, Gasthaus, ... auf einer Bewertungsplattform, trägt sich in einem Gästebuch ein
  - Benutzer verwendet Online-Office-Services oder -Fotobearbeitungsdienste oder ...
  - Benutzer hat Social-Account (auf Facebook, ...) und berichtet
  - Benutzer "zwitschert" über "Gott und die Welt" auf Twitter
  - Benutzer beteiligen sich an einem Themenforum
  - Unternehmen verlagern ihre Dienste in eine "Cloud"
- Links auf fremde Dienste (§ 17)
  - Website verlinkt auf andere (fremde) Websites

VO SS2019 - Juridicum

Ausschluss der Verantwortlichkeit bei Speicherung fremder Inhalte (Hosting)

§ 16. (1) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert, ist für die im Auftrag eines Nutzers gespeicherten Informationen nicht verantwortlich, sofern er
1. von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder,
2. sobald er diese Kenntnis oder dieses Bewusstsein erhalten hat, unverzüglich tätig wird, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

(2) Abs. 1 ist nicht anzuwenden, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Ausschluss der Verantwortlichkeit bei Links

§ 17. (1) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Informationen nicht verantwortlich,
1. sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder,
2. sobald er diese Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen.

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird oder der Diensteanbieter die fremden Informationen als seine eigenen darstellt.

Dienstleister muss bei offensichtlichem Rechtsbruch von sich aus tätig werden, Beispiele: Newsgruppen, Tauschbörsen, Web-Angebote, Praxisbeispiel: eingescannte Landkarten

Verantwortung spezifischer Diensteanbieter IV
(§ 18 für §§ 16-17 ECG)

Keine Verantwortung unter bestimmten Umständen:

1. sofern keine Kenntnis des rechtswidrigen Inhalts und auch keine Umstände bekannt, aus denen der rechtswidrige Inhalt oder Tätigkeit offensichtlich ist oder
2. bei Kenntnis der rechtswidrigen Tatsache unverzügliches tätig werden zum Entfernen des Hinweises/der Inhalte

Erweiterte Auskunftspflichten bei Hosting

⇨ siehe Abschnitt Auskunftspflichten

Aber:

- keine generelle Überwachungspflicht, es müssen keine aktiven Maßnahmen zur Identifikation rechtswidriger Inhalte gesetzt werden
- keine vorbeugenden Aufzeichnungspflichten (es erfolgte auch keine Regelung im Rahmen der Vorratsspeicherung)

Umfang der Pflichten der Diensteanbieter

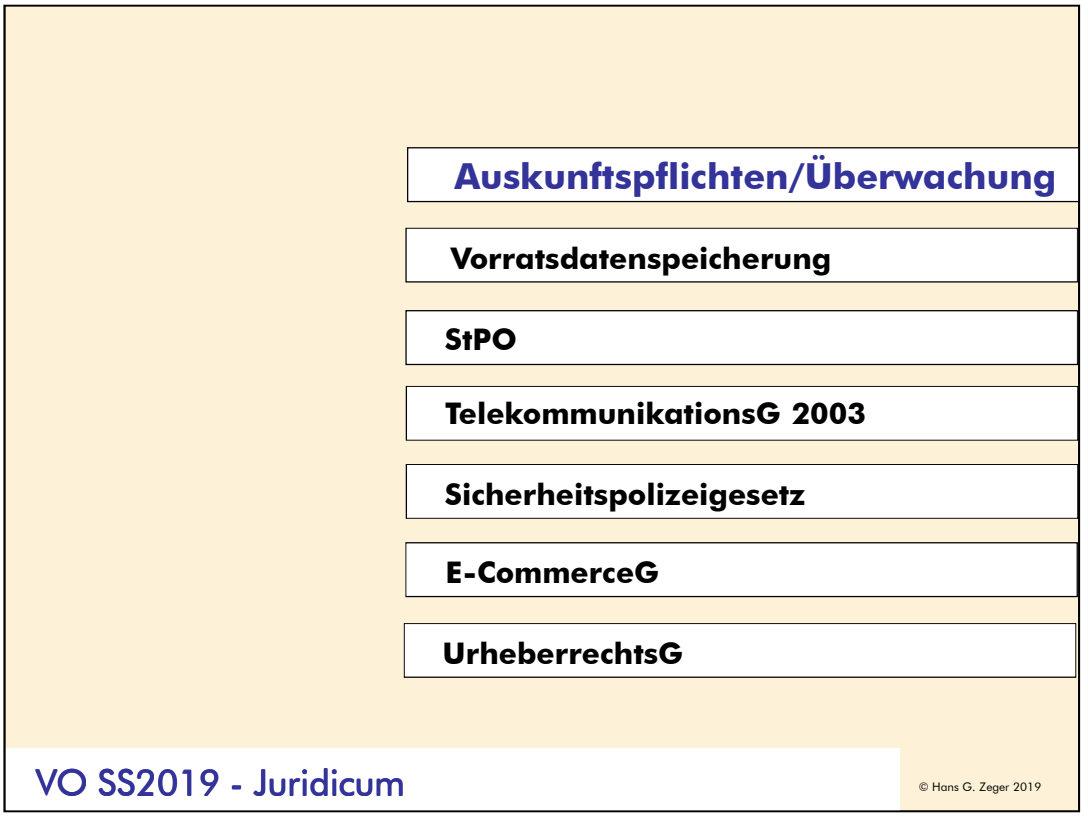
§ 18. (1) Die in den §§ 13 bis 17 genannten Diensteanbieter sind nicht verpflichtet, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.

(2) Die in den §§ 13 und 16 genannten Diensteanbieter haben auf Grund der Anordnung eines dazu gesetzlich befugten inländischen Gerichtes diesem alle Informationen zu übermitteln, an Hand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können.

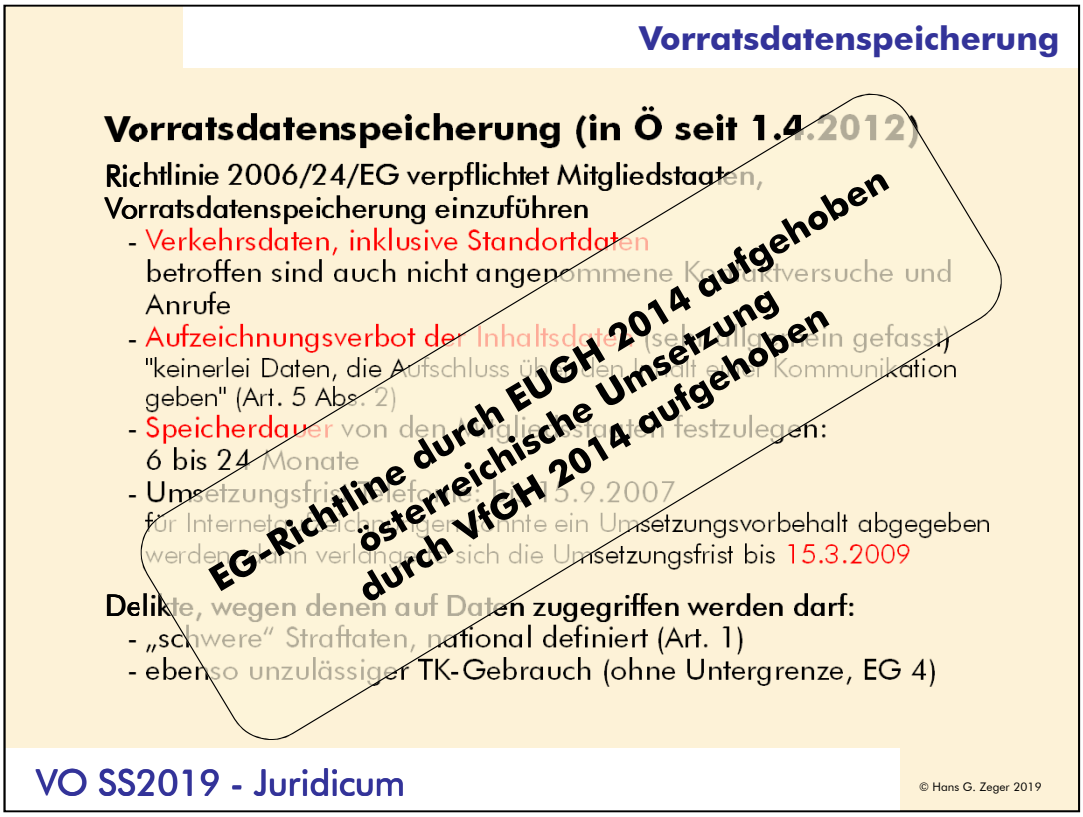
(3) Die in § 16 genannten Diensteanbieter haben auf Grund der Anordnung einer Verwaltungsbehörde dieser den Namen und die Adressen der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgaben bildet.

(4) Die in § 16 genannten Diensteanbieter haben den Namen und die Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

(5) Sonstige Auskunfts- und Mitwirkungspflichten der Diensteanbieter gegenüber Behörden oder Gerichten bleiben unberührt.


Auskunftspflichten/Überwachung
Vorratsdatenspeicherung
StPO
TelekommunikationsG 2003
Sicherheitspolizeigesetz
E-CommerceG
UrheberrechtsG
VO SS2019 - Juridicum
© Hans G. Zeger 2019

-



RICHTLINIE 2006/24/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG

EG (4) In Artikel 15 Absatz 1 der Richtlinie 2002/58/EG ist festgelegt, unter welchen Bedingungen die Mitgliedstaaten die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 der genannten Richtlinie beschränken dürfen. Etwaige Beschränkungen müssen zu besonderen Zwecken der Aufrechterhaltung der öffentlichen Ordnung, d. h. für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des **unzulässigen Gebrauchs von elektronischen Kommunikationssystemen**, in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sein.

Artikel 1 - Gegenstand und Anwendungsbereich

(1) Mit dieser Richtlinie sollen die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter Daten, die von ihnen erzeugt oder verarbeitet werden, harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen.

Artikel 5 - Kategorien von auf Vorrat zu speichernden Daten

...
(2) Nach dieser Richtlinie dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden.

Vorratsdatenspeicherung II

- 1.4.2012: Vorratsdatenspeicherung trat in Österreich in Kraft
- 8.4.2014: Gerichtshof der Europäischen Union hebt die Richtlinie auf (C-293/12, C-594/12)
- 27.6.2014: Verfassungsgerichtshof hebt die österreichischen Bestimmungen auf (G 47/2012)
- Beide Gerichte schließen Vorratsdatenspeicherung nicht völlig aus, sehen aber einen schwerwiegenden und unverhältnismäßigen Eingriff in die Privatsphäre
- Die Bestimmungen wurden ohne Reparaturfrist aufgehoben: weitere Speicherung unzulässig, Daten müssen gelöscht werden
- EU-Kommission will keine neue Richtlinie
- DE: BVerfG hat das deutsche Gesetz schon 2010 aufgehoben, 2015 neues Gesetz beschlossen
- BE, BG, NL, PL, RO, SI, SK, UK: Gerichte haben die Gesetze 2014 oder 2015 aufgehoben

-

Auskunftspflichten / Überwachung StPO

Überwachung gemäß StPO (§§ 134–140)

Formen von Eingriffen im Bereich elektronischer Systeme

- **Fall 1:** "Auskunft über Daten einer Nachrichtenübermittlung"
  § 134 Abs. 2 - auch "äußere Rufdatenerfassung"
  umfasst: "aktuelle" Verkehrs-, Zugangs- und Standortdaten
- **Fall 2:** "Lokalisierung technischer Einrichtungen"
  § 134 Abs. 2a - auch "IMSI-Cacher"
- **Fall 3:** "Überwachung von Nachrichten"
  § 134 Abs. 3 - "[innere] Rufdatenerfassung"
  umfasst: Inhalt von Nachrichten

Anzuwenden auf Telekommunikationsdienste (gem. TKG) oder Dienste der Informationsgesellschaft (gem. Notifikationsgesetz)

Beispiele: Telekomunternehmen (inkl. Mobilfunk), Access-Provider, Mailservice-Anbieter, Forumsbetreiber, "Skype" (VoIP), ...

VO SS2019 - Juridicum

Notifikationsgesetz 1999

§ 1 Z 2. **„Dienst"**: eine Dienstleistung der Informationsgesellschaft, das ist jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, wobei im Sinne dieser Definition bedeuten:

a) **„im Fernabsatz erbrachte Dienstleistung"**: eine Dienstleistung, die **ohne gleichzeitige physische Anwesenheit der Parteien** erbracht wird,

b) „elektronisch erbrachte Dienstleistung": eine Dienstleistung, die mittels **Geräten für die elektronische Verarbeitung**, einschließlich digitaler Kompression, und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen und vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischen Weg gesendet, weitergeleitet und empfangen wird, und

c) **„auf individuellen Abruf eines Empfängers erbrachte Dienstleistung"**: eine Dienstleistung, die durch die **Übertragung von Daten auf individuelle Anforderung** erbracht wird; Anlage 1 enthält eine nicht abschließende Liste jener Dienstleistungen, die nicht unter diese Definition fallen;

StPO § 134 Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten und von Personen

...

2. „Auskunft über Daten einer Nachrichtenübermittlung" die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG), die nicht einer Anordnung gemäß § 76a Abs. 2 unterliegen, und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes),

2a. „Lokalisierung einer technischen Einrichtung" der Einsatz technischer Mittel zur Feststellung von geographischen Standorten und der zur internationalen Kennung des Benutzers dienenden Nummer (IMSI) ohne Mitwirkung eines Anbieters (§ 92 Abs. 3 Z 1 TKG) oder sonstigen Diensteanbieters (§ 13, § 16 und § 18 Abs. 2 des E – Commerce – Gesetzes – ECG, BGBl. I Nr. 152/2001),

2b. „Anlassdatenspeicherung" das Absehen von der Löschung der in Z 2 genannten Daten (§ 99 Abs. 2 Z 4 TKG),

3. „Überwachung von Nachrichten" das Überwachen von Nachrichten und Informationen, die von einer natürlichen Person über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) gesendet, übermittelt oder empfangen werden,

4. „optische und akustische Überwachung von Personen" die Überwachung des Verhaltens von Personen unter Durchbrechung ihrer Privatsphäre und der Äußerungen von Personen, die nicht zur unmittelbaren Kenntnisnahme Dritter bestimmt sind, unter Verwendung technischer Mittel zur Bild- oder Tonübertragung und zur Bild- oder Tonaufnahme ohne Kenntnis der Betroffenen,

...

Vorratsdatenspeicherung + Bundestrojaner

- 1.6.2018: **Vorratsdatenspeicherung "light" eingeführt**
  (fallweise als quick freeze bezeichnet)
  im Anlassfall kann die Löschung von Verkehrsdaten, Zugangsdaten und Standortdaten iS des TKG 2003 untersagt werden ⇨ StPO § 134 Abs. 2a ("Fall 4")
- 1.4.2020: **Eingriffe in Computersysteme vorgesehen**
  (fallweise als Bundestrojaner bezeichnet)
  Installation eines Programms in Computersystem ohne Kenntnis dessen Inhabers um Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden ⇨ StPO § 134 Abs. 3a ("Fall 5")

StPO § 134 (ab 1.4.2020, neu fett)

...

3a. **„Überwachung verschlüsselter Nachrichten" das Überwachen verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten und Informationen im Sinne von Z 3 sowie das Ermitteln damit im Zusammenhang stehender Daten im Sinn des § 76a und des § 92 Abs. 3 Z 4 und 4a TKG durch Installation eines Programms in einem Computersystem (§ 74 Abs. 1 Z 8 StGB) ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter, um eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden,**

...

5. „Ergebnis" (der unter Z 1 bis 4 angeführten Beschlagnahme, Auskunft, Lokalisierung oder Überwachung) der Inhalt von Briefen (Z 1), die Daten einer Nachrichtenübermittlung (Z 2), die festgestellten geographischen Standorte und zur internationalen Kennung des Benutzers dienenden Nummern (IMSI) (Z 2a), die gesendeten, übermittelten oder empfangenen Nachrichten und Informationen (Z 3), **die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen im Sinne von Z 3 sowie damit in Zusammenhang stehende Daten im Sinn des § 76a und des § 92 Abs. 3 Z 4 und 4a TKG (Z 3a)** und die Bild- oder Tonaufnahme einer Überwachung (Z 4).

Auskunftspflichten / Überwachung StPO

Überwachung gemäß StPO (§§ 134–140)

Voraussetzungen für Fall 1 "Rufdaten"
(§ 135 Abs. 2):

- Z 1: Entführungsfall (Verdacht)
- Z 2: vorsätzlich begangene Straftat, Freiheitsstrafe von mehr als sechs Monaten mit Zustimmung des Inhabers der Einrichtung (Aufklärung)
- Z 3,4: vorsätzlich begangene Straftat, Freiheitsstrafe von mehr als ein Jahr (Aufklärung, Fahndung)
- Auskunftszeitraum kann sowohl Zukunft, als auch Vergangenheit umfassen, Verlängerung möglich (§ 137 Abs. 3)

VO SS2019 - Juridicum

Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten

StPO § 135. (1) Beschlagnahme von Briefen ist zulässig, wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist.

(2) Auskunft über Daten einer Nachrichtenübermittlung ist zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird,

2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder

3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.

4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

Auskunftspflichten / Überwachung StPO

Überwachung gemäß StPO (§§ 134–140)

Voraussetzungen für Fall 2 "Lokalisierung"
(§ 135 Abs. 2a):

- Abs. 2 Z 1: Entführungsfall (Verdacht)
- Abs 2 Z 3,4: vorsätzlich begangene Straftat, Freiheitsstrafe von mehr als ein Jahr (Aufklärung, Fahndung)
- Auskunftszeitraum kann sowohl Zukunft, als auch Vergangenheit umfassen, Verlängerung möglich (§ 137 Abs. 3)

VO SS2019 - Juridicum

Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten

StPO § 135.

...

(2a) Lokalisierung einer technischen Einrichtung ist in den Fällen des Abs. 2 Z 1, 3 und 4 ausschließlich zur Feststellung der in § 134 Z 2a genannten Daten zulässig.

...

Auskunftspflichten / Überwachung StPO

Überwachung gemäß StPO (§§ 134–140)

Voraussetzungen für Fall 3 "Inhalte" (§ 135 Abs. 3):

- wie Fall 1: Abs. 2 Z 1 und Z 4
- Abs. 2 Z 2: nur mit Zustimmung des Inhabers
- Abs. 2 Z 3 eingeschränkt: bei vorsätzlich begangener Straftat, Freiheitsstrafe von mehr als ein Jahr erforderlich oder Verhinderung oder Aufklärung im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten strafbaren Handlungen ansonsten wesentlich erschwert wäre und
  a. Inhaber der technischen Einrichtung dringend verdächtig oder
  b. verdächtige Person benutzt die technische Einrichtung oder stellt Verbindung dazu her
- Überwachung kann nur für zukünftigen Zeitraum angeordnet werden (§ 137 Abs. 3)

VO SS2019 - Juridicum

Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten

StPO § 135

...

(3) Überwachung von Nachrichten ist zulässig,

1. in den Fällen des Abs. 2 Z 1,

2. in den Fällen des Abs. 2 Z 2, sofern der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Überwachung zustimmt,

3. wenn dies zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten Straftaten ansonsten wesentlich erschwert wäre und

a. der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, oder einer Straftat gemäß §§ 278 bis 278b StGB dringend verdächtig ist, oder

b. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat (lit. a) dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde;

4. in den Fällen des Abs. 2 Z 4.

Auskunftspflichten / Überwachung StPO

Überwachung gemäß StPO (§§ 134–140)

Voraussetzungen für Fall 4 "quick freeze" (Ergänzung zur Rufdaten-Überwachung)
(§ 135 Abs. 2b)

- Z 2 - 4: sofern zur Sicherung der Überwachung erforderlich

VO SS2019 - Juridicum

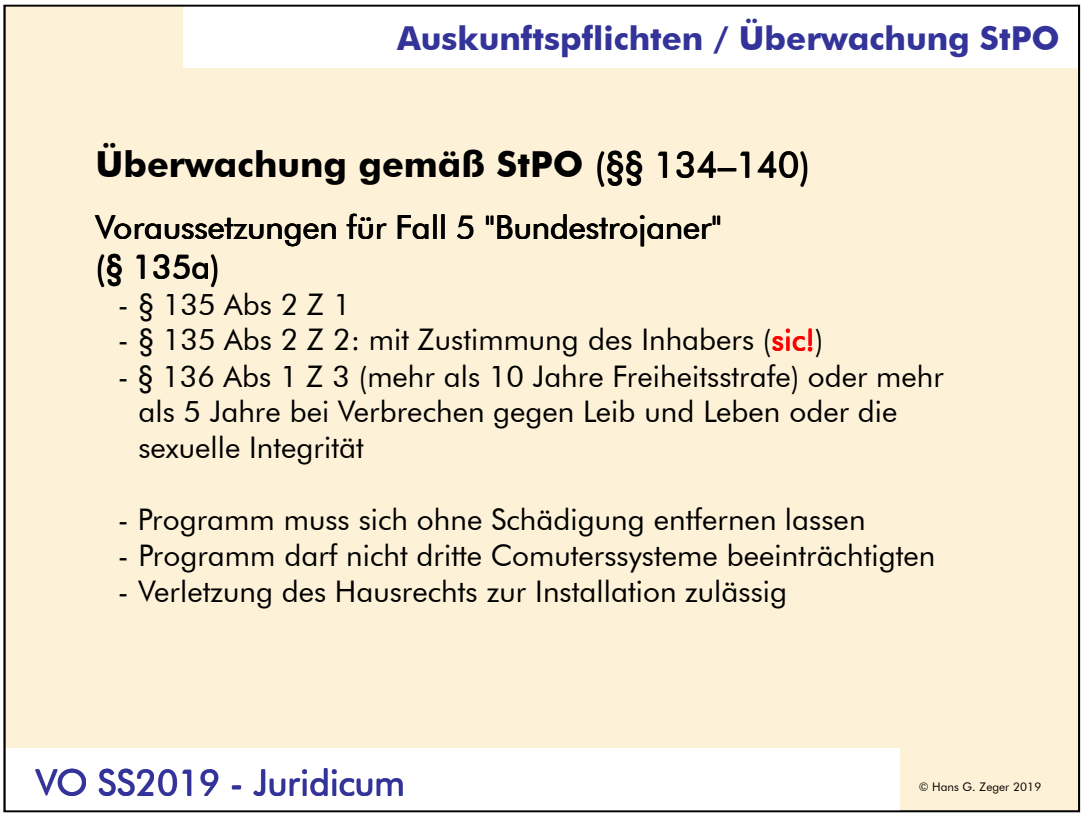
Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten

StPO § 135.

...

(2b) Anlassdatenspeicherung ist zulässig, wenn dies aufgrund eines Anfangsverdachts (§ 1 Abs. 3) zur Sicherung einer Anordnung nach Abs. 2 Z 2 bis 4 oder einer Anordnung nach § 76a Abs. 2 erforderlich erscheint.

...



Überwachung verschlüsselter Nachrichten

§ 135a. (1) Überwachung verschlüsselter Nachrichten ist zulässig:

1. in den Fällen des § 135 Abs. 2 Z 1,

2. in den Fällen des § 135 Abs. 2 Z 2, sofern der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, der Überwachung zustimmt, oder

3. in den Fällen des § 136 Abs. 1 Z 3 sowie wenn die Aufklärung eines mit mehr als fünfjähriger Freiheitsstrafe bedrohten Verbrechens gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung ansonsten aussichtslos oder wesentlich erschwert wäre und

a. der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, einer solchen Straftat dringend verdächtig ist, oder

b. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, benützen oder mit ihm eine Verbindung herstellen werde.

(2) Eine Überwachung verschlüsselter Nachrichten ist überdies nur dann zulässig, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass das Programm

1. nach Beendigung der Ermittlungsmaßnahme funktionsunfähig ist oder ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems, in dem es installiert wurde, und der in ihm gespeicherten Daten entfernt wird, und

2. keine Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme, in denen kein Programm zur Überwachung verschlüsselter Nachrichten installiert wird, bewirkt.

(3) Soweit dies zur Durchführung der Ermittlungsmaßnahme unumgänglich ist, ist es zulässig, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden, um die Installation des Programms zur Überwachung verschlüsselter Nachrichten in dem Computersystem zu ermöglichen. Die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffener sind soweit wie möglich zu wahren.

Auskunftspflichten / Überwachung StPO

Überwachung gemäß StPO (§§ 134–140)

- Von der Staatsanwaltschaft mit gerichtlicher Bewilligung anzuordnen (§ 137 Abs. 1 StPO)
- Mitwirkungs- und Auskunftspflicht für Betreiber nach TKG 2003 und Diensteanbieter nach E-Commerce-Gesetz (§ 138 Abs. 2 StPO) Verpflichtung geregelt in der Überwachungsverordnung (§ 94 TKG 2003), Sprachtelefoniebetreiber mit eigenen physikalischen Anschlüssen müssen spezielle technische Einrichtungen zur Überwachung bereitstellen, ab 1.4.2012 80% Kostenersatz im Zusammenhang mit Vorratsspeicherung, bei allen Unternehmen
- Anspruch auf Kostenersatz (geregelt in der Überwachungskostenverordnung, ÜKVO) **aber:** gilt nur für Telekom-Anbieter, für Diensteanbieter nach ECG weder spezifische Regelungen, noch Kostenersatz vorgesehen

VO SS2019 - Juridicum

Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung - ÜVO) StF: BGBl. II Nr. 418/2001

Verordnung der Bundesministerin für Justiz über den Ersatz der Kosten der Betreiber für die Mitwirkung an der Überwachung einer Telekommunikation (Überwachungskostenverordnung - ÜKVO) StF: BGBl. II Nr. 322/2004

Verpflichtete E-Commerce-Anbieter:

§ 13 ECG: "Access-Provider", "ISP"
Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermitteln oder den Zugang zu einem Kommunikationsnetz vermitteln.

§ 16 ECG: "Hosting-Provider"
Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert.
umfasst etwa Anbieter von Webspace, Webhosts, Serverhousing, Mailservice, Blogservice, Forumsbetreiber, Social Media - Anbieter, ...

Nicht betroffen: Suchmaschinenbetreiber, Caching- oder Proxy-Services

Auskunftspflichten / Überwachung StPO

Überwachung gemäß StPO (§§ 134–140)

- Verständigungspflicht des Beschuldigen (§ 138 Abs 5 StPO)
  aber: kann aufgeschoben werden, wenn dieses oder anderes Verfahren gefährdet ist
- Einsichtsrecht des Beschuldigten in alle für das Verfahren bedeutsamen Ergebnisse (§ 139 Abs. 1 StPO)
- Einsichtsrecht der sonstigen Betroffenen insoweit sie davon betroffen sind, die Betroffenen sind von diesem Recht zu informieren (§ 139 Abs. 2 StPO)
  aber: nur insoweit ihre Identität bekannt oder ohne besonderen Verfahrensaufwand feststellbar ist
- Beweisverwertungbeschränkung, Nichtigkeit bei rechtswidriger Überwachung (§ 140 StPO)
  aber: Verwertung von "Zufallsfunden" zulässig, wenn Überwachungsvoraussetzungen gegeben gewesen wäre

VO SS2019 - Juridicum

-

Auskunftspflichten / Überwachung StPO

Entscheidung zum Auskunftsumfang

OGH Entscheidung 12Os93/14i 5.3.2015

Auskunftsvoraussetzung

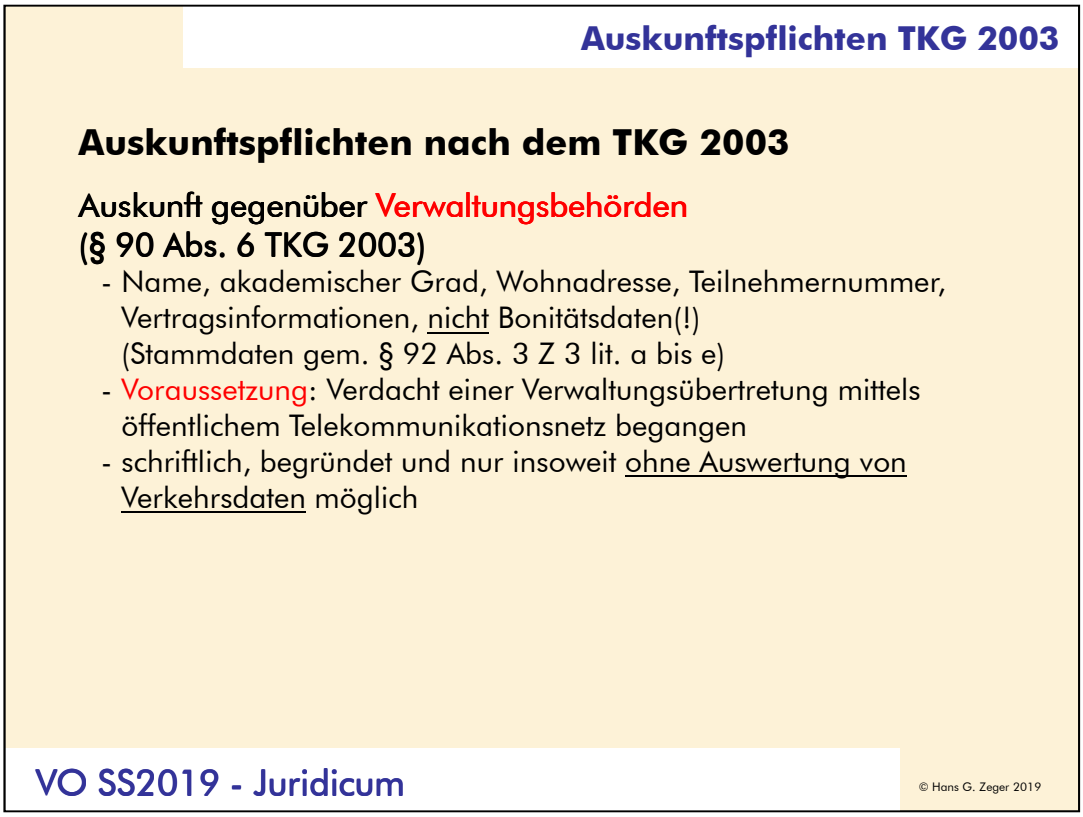
- Auskünfte sind über Kommunikationseinrichtungen zu erteilen
- Unklarheiten in der Interpretation von "technische Einrichtung und das Endgerät " (§ 138 Abs 1 Z 3 StPO)

Entscheidung

- gemeint sind nicht bloß Endeinrichtungen in der Verfügungsgewalt der Benutzer, sondern auch Infrastruktureinrichtungen (Funkeinrichtungen einer Zelle)
- davor unterschiedliche Entscheidungen OLG Linz 9Bs108/13s / OLG Innsbruck 11Bs150/13s, Wien
- **„Funkzellenauswertung" gemäß § 135 Abs 2 StPO zulässig**

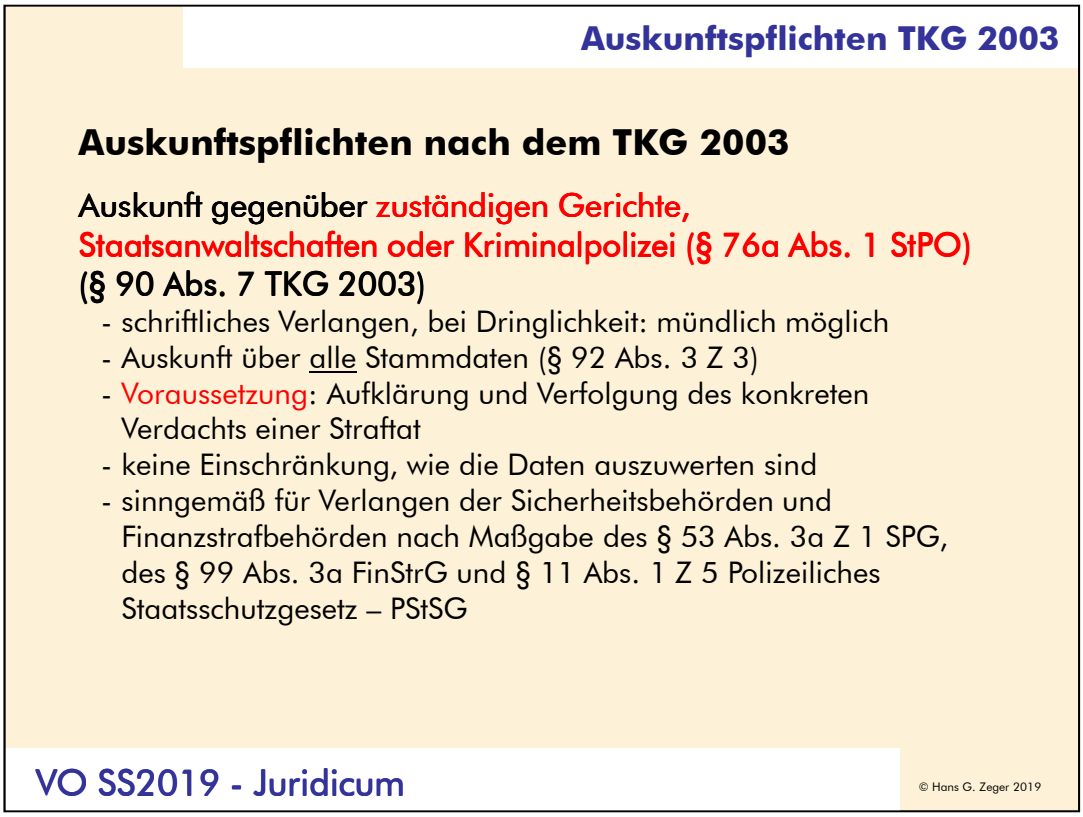
VO SS2019 - Juridicum

-



§ 90 Abs. 6 TKG 2003

Anbieter von Kommunikationsdiensten sind verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über Stammdaten im Sinne von § 92 Abs. 3 Z 3 lit. a bis e von Teilnehmern zu geben, die in Verdacht stehen, durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben, soweit dies ohne Verarbeitung von Verkehrsdaten möglich ist.



§ 90 Abs. 7 TKG 2003

Anbieter von Kommunikationsdiensten sind auf schriftliches Verlangen der zuständigen Gerichte, Staatsanwaltschaften oder der Kriminalpolizei (§ 76a Abs. 1 StPO) verpflichtet, diesen zur Aufklärung und Verfolgung des konkreten Verdachts einer Straftat Auskunft über Stammdaten (§ 92 Abs. 3 Z 3) von Teilnehmern zu geben. Dies gilt sinngemäß für Verlangen der Sicherheitsbehörden und Finanzstrafbehörden nach Maßgabe des § 53 Abs. 3a Z 1 SPG, des § 99 Abs. 3a FinStrG und § 11 Abs. 1 Z 5 Polizeiliches Staatsschutzgesetz – PStSG, BGBl. I Nr. 6/2016. In dringenden Fällen können aber solche Ersuchen vorläufig mündlich übermittelt werden.

Auskunftspflichten nach dem TKG 2003 II

Auskunft an Notrufträger (§ 98 TKG 2003)

- Name, akademischer Grad, Wohnadresse, Teilnehmernummer (Stammdaten gem. § 92 Abs. 3 Z 3 lit. a bis d) + Standortdaten (gem. § 92 Abs. 3 Z 6)
- Standortdaten sind schon bei Rufaufbau bekannt zu geben
- wenn aktuelle Standortdaten nicht feststellbar, dann auch Auskunft über letzte bekannte Cell-ID
- Auskunftserfordernis ist durch Notrufträger zu dokumentieren und unverzüglich, spätestens innerhalb von 24 Stunden dem Betreiber vorzulegen
- Voraussetzung: vorliegen eines Notfalls

Auskünfte an Betreiber von Notrufdiensten § 98 TKG 2003

§ 98. (1) Betreiber eines Kommunikationsnetzes oder -dienstes haben Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Stammdaten im Sinne von § 92 Abs. 3 Z 3 lit. a bis d sowie über Standortdaten im Sinne des § 92 Abs. 3 Z 6 zu erteilen. In beiden Fällen ist Voraussetzung für die Zulässigkeit der Übermittlung ein Notfall, der nur durch Bekanntgabe dieser Informationen abgewehrt werden kann. Die Notwendigkeit der Informationsübermittlung ist vom Betreiber des Notrufdienstes zu dokumentieren und dem Betreiber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nachzureichen. Der Betreiber darf die Übermittlung nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen. Den Betreiber des Notrufdienstes trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens.

(2) Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung zum letzten Kommunikationsvorgang der Endeinrichtung des gefährdeten Menschen verarbeitet werden. Der Anbieter hat den betroffenen Teilnehmer über eine Auskunft über Standortdaten nach dieser Ziffer frühestens nach 48 Stunden, jedoch spätestens nach 30 Tagen grundsätzlich durch Versand einer Kurzmitteilung (SMS), wenn dies nicht möglich ist schriftlich, zu informieren. Diese Information hat zu enthalten:

a) die Rechtsgrundlage,

b) die betroffene Daten,

c) das Datum und die Uhrzeit der Abfrage,

d) Angabe der Stelle, von der die Standortfeststellung in Auftrag gegeben wurde, sowie eine entsprechende Kontaktinformation.

(3) Betreiber gemäß § 20 haben Betreibern von Notrufdiensten unmittelbar nach Eingang eines Notrufes Standortdaten im Sinne des § 92 Abs. 3 Z 6 der Telekommunikationsendeinrichtung, von der aus die Notrufnummer gewählt wurde, zugänglich zu machen und auf Anfrage Auskünfte über Stammdaten gemäß § 92 Abs. 3 Z 3 lit. a bis d zu erteilen.

(4) Betreiber von Kommunikationsnetzen haben bei der Ermittlung des Standortes der Telekommunikationsendeinrichtung entgeltfrei mitzuwirken, soweit hierfür internationale Standards vorhanden sind.

(4a) Betreiber von Kommunikationsnetzen und –diensten haben bei der Übermittlung des endgeräteseitig ermittelten Standortes der Telekommunikationsendeinrichtung entgeltfrei mitzuwirken.

(5) Die Regulierungsbehörde kann mit Verordnung die näheren Details der Ermittlung, insbesondere die Genauigkeit und die Zuverlässigkeit der Standortermittlungen und Übertragung des Standortes der Telekommunikationsendeinrichtung festlegen. Weiters können mit dieser Verordnung Maßnahmen angeordnet werden, welche die Erfassung und die Zurverfügungstellung endgeräteseitig ermittelter Standortdaten an Betreiber von Notrufdiensten ermöglichen. Hierbei hat sie insbesondere auf internationale Standards, grundlegende Anforderungen im öffentlichen Interesse, die technischen Möglichkeiten und die hiefür erforderlichen Investitionen, allfällig bereits bestehende vertragliche Vereinbarungen zwischen Anbietern von Kommunikationsnetzen oder -diensten und Betreibern von Notrufdiensten sowie die Angemessenheit des erforderlichen wirtschaftlichen Aufwandes Bedacht zu nehmen.

Auskunftspflichten SPG

komplexe Auskunftspflichten nach dem SPG

§ 53 Abs. 1 regelt generell Verwendung personenbezogener Daten bei Sicherheitsbehörden, u.a.

- Abwehr krimineller Verbindungen [iS § 16 Abs. 1 Z 2: drei oder mehr Menschen mit dem Vorsatz fortgesetzt gerichtlich strafbare Handlungen zu begehen] (Z 2)
- erweiterte Gefahrenerforschung (Z 2a)
  [z.B. iS § 21 Abs. 3 Z 1 eine einzelne Person, die sich mittels Telekommunikationseinrichtungen für Gewalt ausspricht oder nach Massenvernichtungsmittel recherchiert und bei dem mit Gewalttaten "zu rechnen" ist]
- Abwehr gefährlicher Angriffe [iS § 16 Abs. 3, jedes Offizialdelikt, Anm.] einschließlich notwendige Gefahrenerforschung (Z 3)
- ~~Analyse und Bewertung der Wahrscheinlichkeit einer Gefährdung verfassungsmäßiger Einrichtungen (Z 7)~~
  durch Polizeiliches Staatsschutzgesetz – PStSG ersetzt

VO SS2019 - Juridicum

Zulässigkeit der Verarbeitung

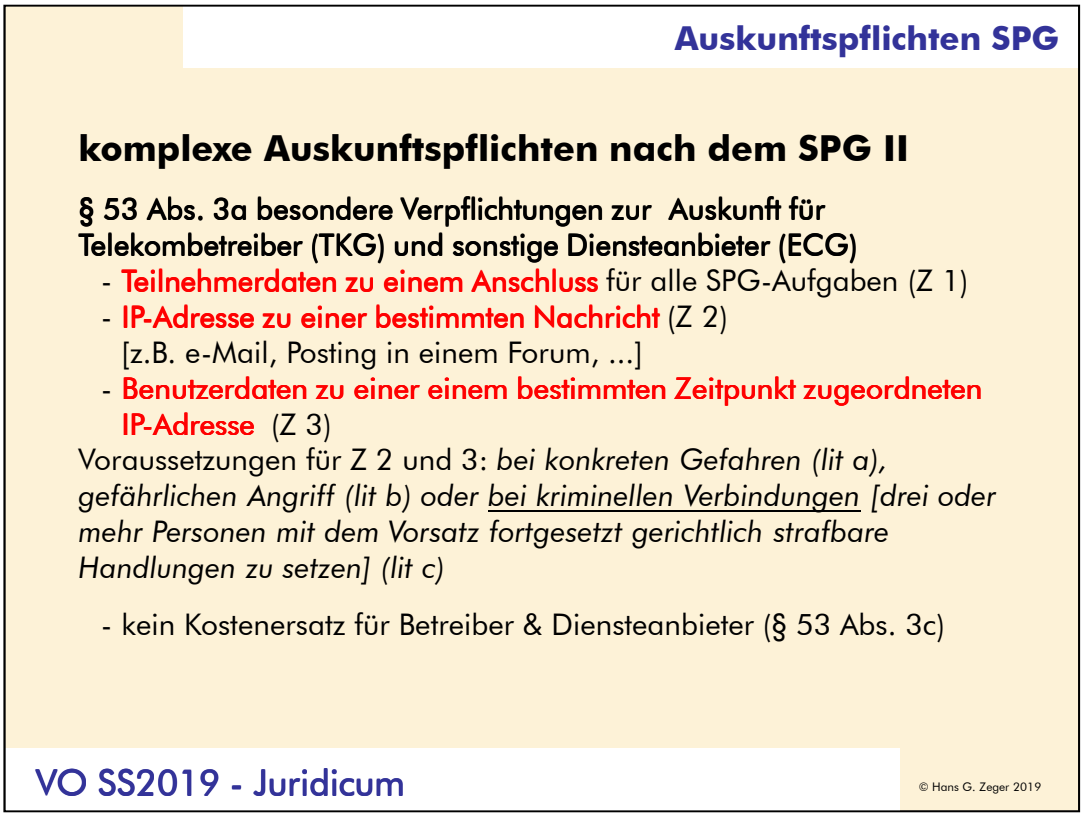
§ 53. (1) Die Sicherheitsbehörden dürfen personenbezogene Daten verarbeiten

1. für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht (§ 19);
2. für die Abwehr krimineller Verbindungen (§§ 16 Abs. 1 Z 2 und 21);

(Anm.: Z 2a aufgehoben durch BGBl. I Nr. 5/2016)

3. für die Abwehr gefährlicher Angriffe (§§ 16 Abs. 2 und 3 sowie 21 Abs. 2); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenerforschung (§ 16 Abs. 4 und § 28a);
4. für die Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt (§ 22 Abs. 2 und 3) oder für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist;
5. für Zwecke der Fahndung (§ 24);
6. um bei einem bestimmten Ereignis die öffentliche Ordnung aufrechterhalten zu können.

(Anm.: Z 7 aufgehoben durch BGBl. I Nr. 5/2016)



SPG § 53

(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70/2003) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskünfte zu verlangen:

1. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses wenn dies zur Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben erforderlich ist,

2. über die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr

a) einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),

b) eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder

c) einer kriminellen Verbindung (§ 16 Abs.1 Z 2) benötigen,

3. über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr

a) einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§19),

b) eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder

c) einer kriminellen Verbindung (§ 16 Abs. 1 Z 2) benötigen,

4. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer, wenn dies zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr gefährlicher Angriffe erforderlich ist.

Auskunftspflichten SPG

komplexe Auskunftspflichten nach dem SPG III

§ 53 Abs. 3b besondere Verpflichtungen zur Auskunft für Telekombetreiber (TKG)

- bei gegenwärtiger Gefahr für Leben oder Gesundheit ("Lawinen- und Selbstmörderbestimmung")

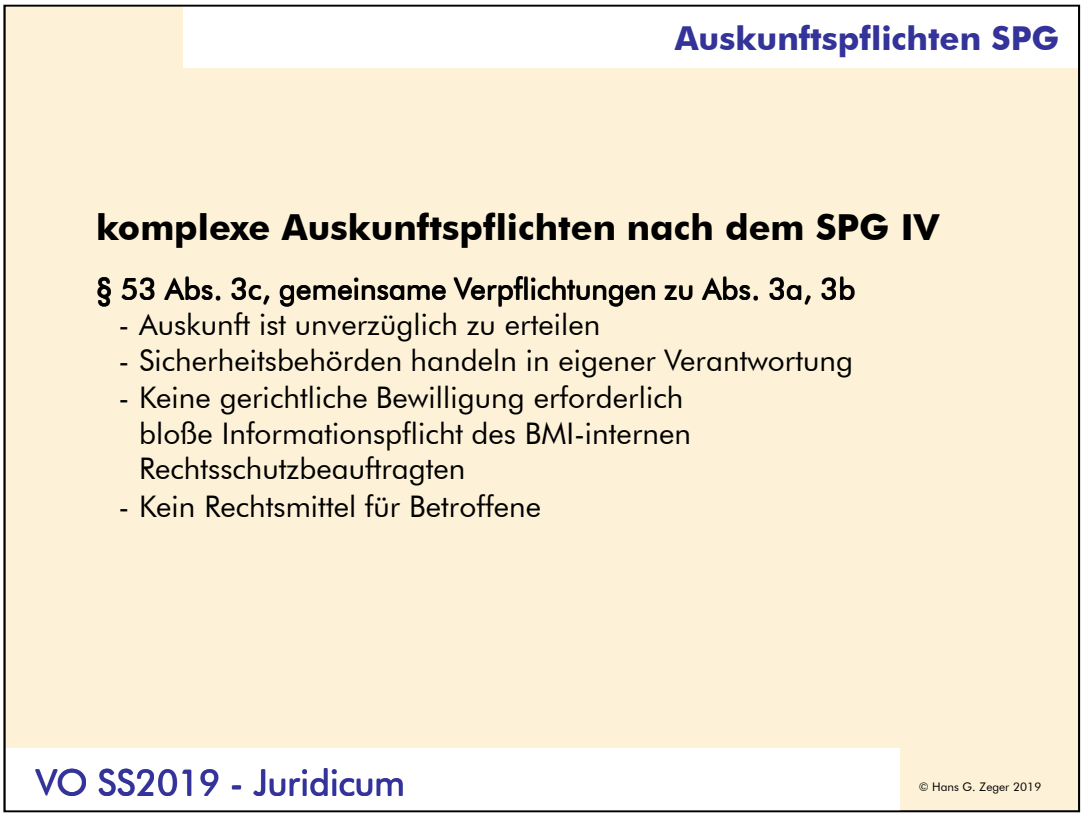
Auskunftsumfang

- Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung
- Sicherheitsbehörde darf technische Mittel zur Lokalisierung der Endeinrichtung einsetzen ("IMSI-Catcher")
- Kostenersatz für Diensteanbieter gem. ÜKVO (§ 53 Abs. 3c)

VO SS2019 - Juridicum

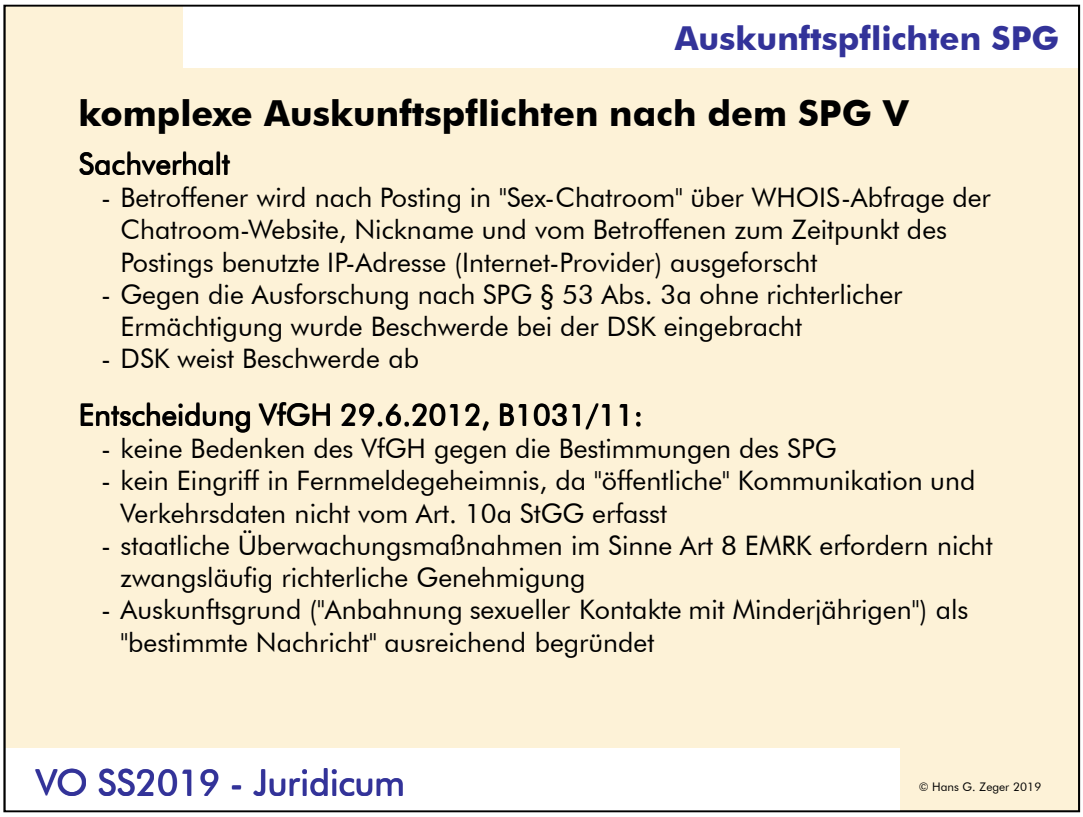
SPG § 53

(3b) Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der vom Gefährder oder von dem gefährdeten oder diesen begleitenden Menschen mitgeführten Endeinrichtung zu verlangen sowie technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz zu bringen.



SPG § 53

(3c) In den Fällen der Abs. 3a und 3b trifft die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens. Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und im Fall des Abs. 3b gegen Ersatz der Kosten nach der Überwachungskostenverordnung – ÜKVO, BGBl. II Nr. 322/2004, zu erteilen. Im Falle des Abs. 3b hat die Sicherheitsbehörde dem Betreiber überdies unverzüglich, spätestens innerhalb von 24 Stunden eine schriftliche Dokumentation nachzureichen. In den Fällen des Abs. 3a Z 3 sowie Abs. 3b ist die Sicherheitsbehörde verpflichtet, den Betroffenen darüber zu informieren, dass eine Auskunft zur Zuordnung seines Namens oder seiner Anschrift zu einer bestimmten IP-Adresse (§ 53 Abs. 3a Z 3) oder zur Standortbeauskunftung (§ 53 Abs. 3b) eingeholt wurde, sofern hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 oder 4 iVm § 102a TKG 2003 erforderlich war. Dabei sind dem Betroffenen nachweislich und ehestmöglich die Rechtsgrundlage sowie das Datum und die Uhrzeit der Anfrage bekannt zu geben. Die Information Betroffener kann aufgeschoben werden, solange durch sie der Ermittlungszweck gefährdet wäre, und kann unterbleiben, wenn der Betroffene bereits nachweislich Kenntnis erlangt hat oder die Information des Betroffenen unmöglich ist.



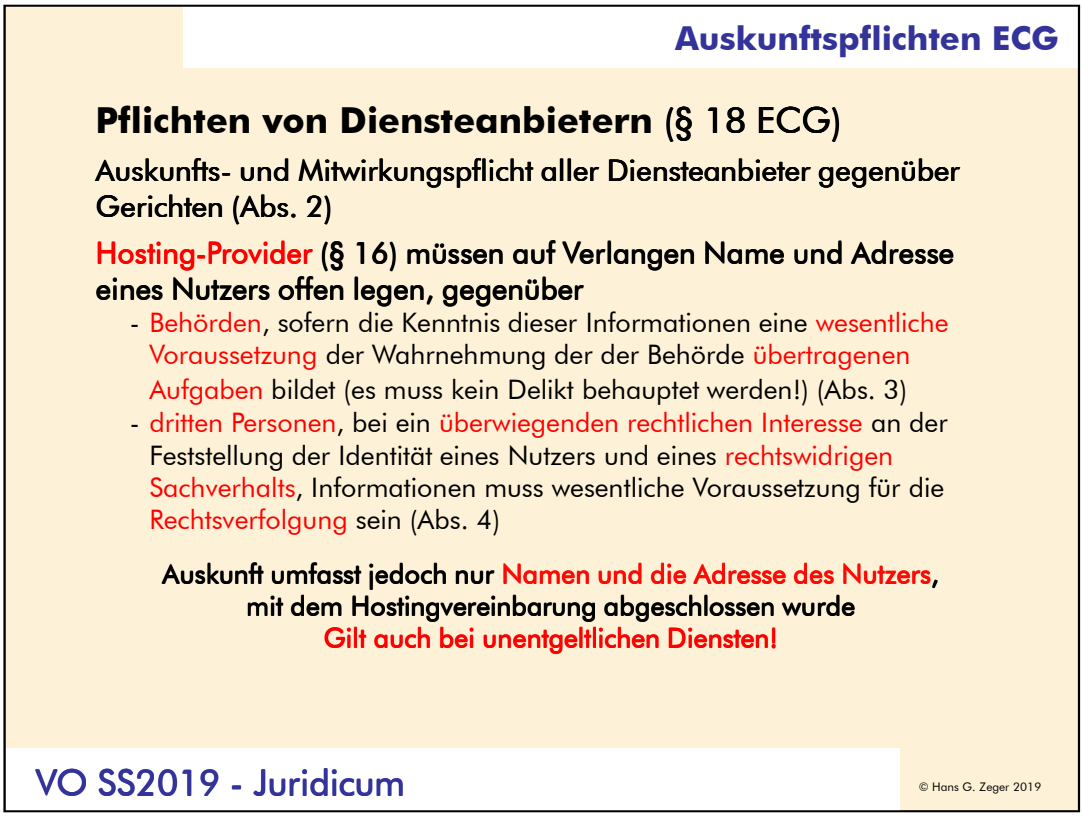
VfGH-Entscheidung B1031/11

Auskunft über Nutzer einer IP-Adresse im Rahmen des SPG zulässig
B-VG Art7 Abs1 / Verwaltungsakt EMRK Art8 DSG 2000 §1 SicherheitspolizeiG §53 Abs3a StGG Art10a TelekommunikationsG 2003 §92, §99 E-Commerce-G §3, §18 StGB §214

Leitsatz
Keine Bedenken gegen Bestimmungen des Sicherheitspolizeigesetzes über die Ermächtigung der Sicherheitsbehörden zur Ermittlung der IP-Adresse sowie des Namens und der Anschrift des Inhabers zur Erfüllung sicherheitspolizeilicher Aufgaben; kein Eingriff in das Fernmeldegeheimnis; keine Ermächtigung zur Ermittlung von Inhaltsdaten; kein Verstoß gegen das Recht auf Datenschutz; keine Verletzung verfassungsgesetzlich gewährleisteter Rechte durch Abweisung einer Beschwerde durch die Datenschutzkommission; vertretbare Annahme einer Gefahr für die Sicherheit Unmündiger angesichts des Internetauftritts des Beschwerdeführers in einem auf sexuelle Kontakte spezialisierten Chatroom

Sachverhalt

1. Der Beschwerdeführer kommunizierte am 11. November 2009 im Internet von seinem PC aus unter einem Benutzernamen ("Nickname") in einem auf sexuelle Kontakte spezialisierten Chatroom mit der ihm zugeteilten Internetprotokolladresse (IP-Adresse). Hiebei erweckte er bei einem Chatpartner den Eindruck, unmündige Personen, nämlich "7-11jährige, oder wenn gewünscht auch jünger", zu sexuellen Handlungen anzubieten. Von diesem Sachverhalt wurde das Landeskriminalamt Wien unter Bekanntgabe der Internetseite (domain) und des vom Beschwerdeführer verwendeten "Nickname" informiert. Die befassten Beamten der Bundespolizeidirektion Wien (BPD Wien) gingen von einer konkret und unmittelbar drohenden Gefahr für die Sicherheit Unmündiger aus und ermittelten zunächst auf Grundlage des §53 Abs3a Z2 des Bundesgesetzes über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG), BGBl. 566/1991 idF BGBl. I 114/2007, im Wege einer sogenannten Whois-Abfrage beim Domaininhaber die Website, sodann anhand dieser und des "Nickname" über den technischen Betreiber des Chatservers die konkrete IP-Adresse des Endgerätes, von dem aus die Nachricht versendet wurde, samt Login-Zeitpunkt. Auf Grund dieser Daten konnte gemäß §53 Abs3a Z3 SPG im Wege einer weiteren Whois-Abfrage der Provider, dem die IP-Adresse (innerhalb eines Adressenblocks) zugeordnet war (UPC Austria GmbH), und über diesen schließlich Namen und Adresse des Beschwerdeführers (als Anschlussinhaber und Benutzer) ausgeforscht werden. Er und eine Reihe weiterer Personen wurden wegen des Verdachts der versuchten Bestimmung zum schweren sexuellen Missbrauch von Unmündigen sowie zur entgeltlichen Förderung fremder Unzucht (§§15, 12 iVm §206 und §214 StGB) bei der Staatsanwaltschaft Wien zur Anzeige gebracht.



Umfang der Pflichten der Diensteanbieter

§ 18. (1) Die in den §§ 13 bis 17 genannten Diensteanbieter sind nicht verpflichtet, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.

(2) Die in den §§ 13 und 16 genannten Diensteanbieter haben auf Grund der Anordnung eines dazu gesetzlich befugten inländischen Gerichtes diesem alle Informationen zu übermitteln, an Hand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können.

(3) Die in § 16 genannten Diensteanbieter haben auf Grund der Anordnung einer Verwaltungsbehörde dieser den Namen und die Adressen der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgaben bildet.

(4) Die in § 16 genannten Diensteanbieter haben den Namen und die Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

(5) Sonstige Auskunfts- und Mitwirkungspflichten der Diensteanbieter gegenüber Behörden oder Gerichten bleiben unberührt.

Auskunftspflichten ECG

Entscheidungen zur Auskunftspflicht
gemäß § 18 ECG

OGH 6 Ob 104/11d 14.9.2011
- die Identität (= Vorname, Zuname, Postanschrift, auch E-Mail-Adresse sind bekannt zu geben
- nur insoweit vorhanden, keine Verpflichtung vorbeugend (für zukünftige Auskunftspflichten) diese Daten zu erheben bzw. vorrätig zu halten

OGH 6 Ob 119/11k 22.6.2012
- wenn Provider nur die dynamische IP-Adresse kennt, sonst nichts, muss er nichts offen legen

OGH 6 Ob 133/13x 23.01.2014, OGH 6 Ob 58/14v, 10.04.2014
- Auskunftspflicht im Spannungsfeld zu Redaktionsgeheimnis
- nicht moderierte Foren und Postings von Online-Benutzern fallen nicht unter Redaktionsgeheimnis, weil Postings "völlig ohne journalistische Kontrolle und Bearbeitung und aus eigenen Antrieb des Nutzers veröffentlicht werden"
- Userdaten sind daher bekannt zu geben

VO SS2019 - Juridicum

-

Entscheidungen zur Auskunftspflicht II

OGH 6 Ob 188/14m, 15.12.2014

- Auch wenn Postings von einem Computerprogramm vor Veröffentlichung geprüft werden, reicht das nicht aus, den erforderlichen Zusammenhang mit einer journalistischen Tätigkeit herzustellen

⇨ Redaktionen reagieren unterschiedlich darauf, Standard hat - schrittweise - eine immer stärkere Moderation eingeführt (inkl. Zensurvorwurf einiger Poster)

-

Zusammenfassung zu den Auskunftspflichten

Keine der genannten Auskunfts- und Überwachungspflichten verpflichtet dazu (vorbeugend) Daten auf Vorrat zu erheben oder zu speichern

Im Gegenteil:

- Nach DSGVO sind Daten zu löschen, wenn sie nicht mehr für den ursprünglichen Zweck benötigt werden
- Konkreter: Nach TKG sind Verkehrsdaten zu löschen, wenn sie nicht mehr für die Verrechnung benötigt werden
- Empfehlung der DSK vom 11.10.2006: Unzulässigkeit der Speicherung von dynamischen IP-Adressen bei Flatrate (K213.000/0005-DSK/2006)

Grundrecht auf Datenschutz ("Geheimhaltung der persönlichen Lebensführung") wird als höherwertig angesehen als die Schaffung von Instrumenten der präventiven Rechtsverfolgung

Vorratsdatenspeicherung "light" relativiert jedoch diese Regelung

-

Überblick / Zusammenfassung

Datenschutzfragen in Internet/eCommerce I

Vorfrage: Handelt es sich um personenbezogene Daten?

Identifizierbarkeit reicht jedoch aus!

(1) Welche Bestimmung ist anwendbar?

a) Telekommunikationsgesetz (setzt bestimmte Technik voraus)

b) andere Spezialbestimmungen (Medienrecht, E-Government-Gesetz, Gesundheitsdatentelematikgesetz, ...)

c) Datenschutzgesetz (setzt Datenverarbeitung voraus)

a) + b) verweisen in Teilen meist auf c)

d) Privatsphärebestimmung (Auffangbestimmung)

(2) Prüfung der Rechtmäßigkeit verwendeter Daten

a) prüfen ob Datenverarbeitung iS DSGVO

b) wenn Datenverarbeitung, drei Schritte: berechtigter Zweck der Datenverarbeitung, Erlaubnis zur Verwendung bestimmter Daten, Registrierungsanforderung

VO SS2019 - Juridicum

-

Überblick / Zusammenfassung

Datenschutzfragen in Internet/eCommerce II

(2) Prüfung der Rechtmäßigkeit verwendeter Daten

...

c) mögliche Rechtsverletzungen nach DSGVO, TKG 2003, Medienrecht, StGB, Privatsphärebestimmungen, UWG, ...

(3) bestehen berechtigte Auskunftspflichten?

a) gemäß StPO, TKG, SPG, ECG, UrhG?, ...

b) gegenüber Gerichten, Sicherheits-, Verwaltungsbehörden, Dritten (Privaten)

c) Umfang der Auskunftspflicht:

- bestimmte Daten / Datenarten,
- Mitwirkungspflicht,
- in bestimmten Fällen hat der Verarbeiter technische Einrichtungen zur Informaitonsweitergabe bereit zu stellen,
- umfasst bestehende Daten

VO SS2019 - Juridicum

-

Resume

Datenschutzfragen in Internet/eCommerce III

- DSGVO ist für globalisiertes Internet extrem komplex, Zweifel an der Praxistauglichkeit sind angebracht
- DSGVO erlaubt "kreativen" Internet-Unternehmen zahlreiche neue Betätigungsmöglichkeiten
- Konflikt zwischen Meinungsfreiheit, Transparenz und Datenschutz wurde verschärft (und wird sich weiter verschärfen)
- EuGH entscheidet eher datenschutzfreundlich (EU-Grundrechtecharta)
- EGMR entscheidet eher in Richtung Meinungsfreiheit (EMRK)

VO SS2019 - Juridicum

-

Ich danke für Ihre Aufmerksamkeit

VO SS2019 - Juridicum

-